[19]中华人民共和国专利局

[51]Int.Cl[6]
H04L 9/20

[12] 发明专利申请公开说明书

[21] 申请号 97114947.X

[43]公开日 1998 年 1 月 21 日

[11] 公开号 CN 1170995A

[22]申请日 97.5.22

[30]优先权

[32]96.5.22 [33]JP[31]126751 / 96

[71]申请人 松下电器产业株式会社

地址 日本大阪府

[72]发明人 松崎夏生 原田俊治 馆林诚

[74]专利代理机构 中国专利代理(香港)有限公司

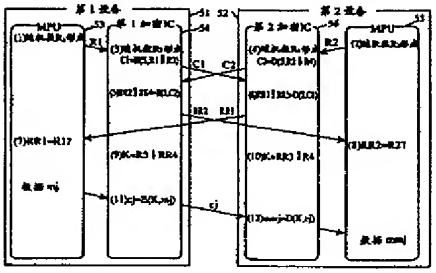
代理人 叶恺东 王忠忠

权利要求书 8 页 说明书 24 页 附图页数 11 页

[54]发明名称 保证设备之间通信安全的加密装置

[57]摘要

在第 1 设备 51 中，MPU53 形成作为询问数据的随机数 R1，第 1 加密 IC54 将上述随机数 R1 和本身形成的数据传送键用的随机数 R3 结合并加密，之后作为密码文字 C1 发送给第 2 设备 52。同样，当接收第 2 设备 52 发送的密码文字 C2 时，第 1 加密 IC54 对上述密码文字 C2 进行译码，将其分成第 1 分离数据 RR2 和第 2 分离数据 RR4。第 1 加密 IC54 将第 1 分离数据 RR2 作为响应数据返回给第 2 设备 52。MPU53 对第 2 设备 52 返回的第 1 分离数据 RR1 和随机数 R1 进行比较，在它们保持一致的场合，认证第 2 设备 52 为正当的设备。



权 利 要 求 书

1. 一种加密装置，它设置于可进行数据传送键的共用、以及采用该数据传送键的数据密码通信的设备中，它包括:

第 1 随机数形成机构，该机构形成用于上述数据传送键的共用的第 1 随机数;

第 1 随机数保持机构，该机构保持所形成的第 1 随机数;

第 1 发送机构，该机构将所形成的第 1 随机数发送给对方设备，在这里，上述对方设备为构成上述密码通信对方的设备;

数据传送键形成机构，该机构采用在上述第 1 随机数保持机构中所保持的第 1 随机数形成随时间变化的上述数据传送键;

传送数据加密机构，该机构采用上述数据传送键对构成密码通信的对象的传送数据进行加密;

在这里，上述第 1 随机数形成机构、上述第 1 随机数保持机构、上述数据传送键形成机构和上述传送数据加密机构由 1 个 IC 内部的电路形成;

上述第 1 随机数保持机构将上述第 1 随机数保存于从上述 IC 外部不可访问的区域。

2. 根据权利要求 1 所述的装置，其特征在于它还包括:

第 1 加密机构，该机构对上述第 1 随机数进行加密;

在这里，上述第 1 加密机构由上述 IC 内部的电路形成;

上述第 1 发送机构将通过上述第 1 随机数加密机构加密的第 1 随机数发送给上述对方设备;

3. 根据权利要求 2 所述的装置，其特征在于上述设备通过根据询问响应型的认证协议的通信相互对上述对方设备是正当的设备进行认证，上述加密装置还包括:

第 2 随机数形成机构，该机构形成发送给上述对方设备的询问数据用的第 2 随机数;

认证机构，该机构对下述的响应数据和上述第 2 随机数是否一致进行判断，该响应数据是由上述对方设备对上述询问数据给出的返回数据，在它们保持一致的场合认证上述对方设备是正当的设备;

在这里，上述数据传送键形成机构在进行上述认证的场合形成上述数据传送键。

4. 根据权利要求 3 所述的装置，其特征在于上述第 2 随机数形成机构和上述认证机构由上述 IC 外部的电路形成。

5. 根据权利要求 4 所述的装置，其特征在于该装置还包括:

译码机构，该机构对上述对方设备发送出的加密的结合数据进行译码;

分离机构，该机构将译码的结合数据分离成与响应相当的第 1 分离数据以及剩余的第 2 分离数据;

第 2 发送机构，该机构将上述第 1 分离数据返回给上述对方设备;

在这里，上述第 1 加密机构将上述第 1 随机数和上述第 2 随机数结合，对所得到的结合数据进行加密;

上述数据传送键形成机构通过将上述第 1 随机数和上述第 2 分离数据结合来形成上述数据传送键;

上述译码机构和上述分离机构由上述 IC 内部的电路形成。

6. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和上述译码机构中的至少一个相同。

7. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和上述译码机构中的任何一个均不相同，并且比它们中的任何一个简单。

8. 根据权利要求 7 所述的装置，其特征在于上述传送数据加密机构将上述传送数据分为具有一定长度的块，采用与上述数据传送键相对应的部分对每个块进行加密。

9. 根据权利要求 8 所述的装置，其特征在于上述传送数据加密机构通过求出上述块和与上述数据传送键相对应的部分的异或的方式进行上述的加密。

10. 根据权利要求 9 所述的装置，其特征在于在上述第 1 加密机构中进行的加密和在上述译码机构中进行的译码采用相同的变换算法。

11. 根据权利要求 10 所述的装置，其特征在于上述第 1 加密机构和上述译码机构采用预先保持于上述 IC 内部的键数据进行上述加密和译码;

上述键数据的一部分存储于上述 IC 内部的屏蔽 ROM 区域，剩余的部分存储于 IC 内部的附加 ROM 区域中。

12. 根据权利要求 4 所述的装置，其特征在于该装置还包括:

第 2 发送机构，该机构将上述第 2 随机数作为询问数据发送给上述对方设备;

译码机构，该机构对由上述对方设备发送来的加密的结合数据进行译码;

分离机构，该机构将译码的结合数据分离成与响应数据相当的第 1 分离数据以及剩余的第 2 分离数据;

在这里，上述认证机构将上述第 1 分离数据作为由上述对方设备返回的响应数据进行判断和认证;

上述第 1 加密机构将由上述对方设备发送来的响应数据与上述第 1 随机数结合，对所得到的结合数据进行加密;

上述数据传送键形成机构通过将上述第 1 随机数和上述第 2 分离数据结合来形成上述数据传送键;

上述译码机构和上述分离机构由上述 IC 内部的电路形成。

13. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和上述译码机构中的至少一个相同。

14. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和上述译码机构中的任何一个均不相同，并且比它们中的任何一个简单。

15 根据权利要求 7 所述的装置，其特征在于上述传送数据加密机构将上述传送数据分为具有一定长度的块，采用与上述数据传送键相对应的部分对每个块进行加密。

16. 根据权利要求 8 所述的装置，其特征在于上述传送数据加密机构通过求出上述块和与上述数据传送键相对应的部分的异或的方式进行上述的加密。

17. 根据权利要求 9 所述的装置，其特征在于在上述第 1 加密机构中进行的加密和在上述译码机构中进行的译码采用相同的变换算法。

18. 根据权利要求 10 所述的装置，其特征在于上述第 1 加密机构和上述译码机构采用预先保持于上述 IC 内部的键数据进行上述加密和译码;

上述键数据的一部分存储于上述 IC 内部的屏蔽 ROM 区域，剩余的部分存储于 IC 内部的附加 ROM 区域中。

19. 根据权利要求 2 所述的装置，其特征在于上述设备通过根据询问响应型

的认证协议的通信相互对上述对方设备是正当的设备进行认证，上述加密装置还包括:

译码机构，该机构对上述对方设备根据上述询问数据而发送出的加密的结合数据进行译码;

分离机构，该机构将译码的结合数据分离成与响应数据相当的第 1 分离数据以及剩余的第 2 分离数据;

认证机构，该机构对上述第 1 随机数与上述第 1 分离数据是否一致进行判断，在它们保持一致的场合，认证上述对方设备为正当的设备;

第 2 加密机构，该机构在形成上述认证的场合对上述第 2 分离数据进行加密;

第 2 发送机构，该机构将加密的上述第 2 分离数据作为响应数据返回给上述对方设备;

在这里，上述数据传送键形成机构通过将上述第 1 随机数和上述第 2 分离数据结合来形成上述数据传送键;

上述译码机构、上述分离机构和上述第 2 加密机构由上述 IC 内部的电路形成。

20. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和第 2 加密机构和上述译码机构中的至少一个相同。

21. 根据权利要求 5 所述的装置，其特征在于上述传送数据加密机构所采用的加密算法与上述第 1 加密机构和第 2 加密机构和上述译码机构中的任何一个均不相同，并且比它们中的任何一个简单。

22. 根据权利要求 7 所述的装置，其特征在于上述传送数据加密机构将上述传送数据分为具有一定长度的块，采用与上述数据传送键相对应的部分对每个块进行加密。

23. 根据权利要求 8 所述的装置，其特征在于上述传送数据加密机构通过求出上述块和与上述数据传送键相对应的部分的异或的方式进行上述的加密。

24. 根据权利要求 9 所述的装置，其特征在于在上述第 1 加密机构和第 2 加密机构中进行的加密和在上述译码机构中进行的译码采用相同的变换算法。

25. 根据权利要求 10 所述的装置，其特征在于上述第 1 加密机构和第 2 加密机构和上述译码机构采用预先保持于上述 IC 内部的键数据进行上述加密和译码;

上述键数据的一部分存储于上述 IC 内部的屏蔽 ROM 区域，剩余的部分存储于 IC 内部的附加 ROM 区域中。

26. 一种通信系统，它由可进行数据传送键的共用以及采用该数据传送键的密码通信的发送机和接收机构成;

上述发送机和接收机通过根据询问响应型的认证协议的通信相互对上述对方设备是正当的设备进行认证;

其分别包括:

第 1 随机数形成机构，该机构形成询问数据用的第 1 随机数;

第 2 随机数形成机构，该机构形成上述数据传送键用的第 2 随机数;

结合机构，该机构将上述第 1 随机数和上述第 2 随机数结合;

加密机构，该机构对上述结合数据进行加密;

第 1 发送机构，该机构将加密的上述结合数据发送给上述对方设备;

第 1 接收机构，该机构接收由上述对方设备的第 1 发送机构发送出的加密的结合数据;

译码机构，该机构对所接收的上述结合数据进行译码;

分离机构，该机构将译码出的上述结合数据分离成与响应数据相当的第 1 分离数据以及上述数据传送键用的第 2 分离数据;

第 2 发送机构，该机构将上述第 1 分离数据作为响应数据返回给上述对方设备;

第 2 接收机构，该机构接收上述对方设备的第 2 接收机构返回的第 1 分离数据;

比较机构，该机构对所接收的上述第 1 分离数据和上述第 1 随机数进行比较，在它们保持一致的场合，认证上述对方设备为正当的设备;

数据传送键形成机构，该机构通过将上述第 2 随机数和上述第 2 分离数据结合来形成上述数据传送键;

密码通信机构，该机构在进行上述认证的场合，采用所形成的上述数据传送键同上述对方设备进行密码通信。

27. 一种通信系统，它由可进行数据传送键的共用以及采用该数据传送键的密码通信的发送机和接收机构成；

上述发送机和接收机通过根据询问响应型的认证协议的通信相互对上述对方设备是正当的设备进行认证；

其分别包括：

第 1 随机数形成机构，该机构形成询问数据用的第 1 随机数；

第 1 发送机构，该机构将上述第 1 随机数发送给上述对方设备；

第 1 接收机构，该机构接收由上述对方设备的第 1 发送机构发送出的第 1 随机数；

第 2 随机数形成机构，该机构形成上述数据传送键用的第 2 随机数；

结合机构，该机构将所接收的上述第 1 随机数和上述第 2 随机数结合；

加密机构，该机构对上述结合数据进行加密；

第 2 发送机构，该机构将加密的上述结合数据返回给上述对方设备；

第 2 接收机构，该机构接收由上述对方设备的第 2 发送机构发送出的加密结合数据；

译码机构，该机构对所接收的上述结合数据进行译码；

分离机构，该机构将译码的上述结合数据分离成与响应数据相当的第 1 分离数据以及上述数据传送键用的第 2 分离数据；

比较机构，该机构对上述第 1 分离数据和通过上述第 1 随机数形成机构所形成的上述第 1 随机数进行比较，在它们保持一致的场合，认证上述对方设备为正当的设备；

数据传送键形成机构，该机构通过将上述第 2 随机数和上述第 2 分离数据结合来形成上述数据传送键；

密码通信机构，该机构在进行上述认证的场合，采用所形成的上述数据传送键，同上述对方设备进行密码通信。

28. 一种通信系统，它由可进行数据传送键的共用以及采用该数据传送键的密码通信的发送机和接收机构成；

上述发送机和接收机通过根据询问响应型的认证协议的通信相互对上述对方设备是正当的设备进行认证；

该发射机包括：

形成第 1 随机数的第 1 随机数形成机构;

对上述第 1 随机数进行加密的第 1 加密机构;

将加密的上述第 1 随机数发送给接收机的第 1 发送机构;

该接收机包括:

接收加密的上述第 1 随机数的第 1 接收机构;

对所接收的上述第 1 随机数进行译码的第 1 译码机构;

形成第 2 随机数的第 2 随机数形成机构;

通过将上述第 1 随机数和上述第 2 随机数结合来形成结合数据的第 1 结合机构;

对上述结合数据进行加密的第 2 加密机构;

将加密的上述结合数据发送给发送机的第 2 发送机构;

上述发送机还包括:

接收加密的上述结合数据的第 2 接收机构;

对所接收的上述结合数据进行译码的第 2 译码机构;

分离机构，该机构将译码的上述结合数据分离成与上述第 1 随机数相当的第 1 分离数据以及与上述第 2 随机数相当的第 2 分离数据;

第 1 比较机构，该机构对上述第 1 随机数和上述第 1 分离数据进行比较，在它们保持一致的场合，认证上述接收机为正当的设备;

第 3 加密机构，该机构在进行上述认证的场合对上述第 2 分离数据进行加密;

第 3 发送机构，该机构将加密的上述第 2 分离数据发送给上述接收机;

第 1 数据传送键形成机构，该机构通过将借助上述第 1 随机数形成机构形成的上述第 1 随机数和借助上述分离机构形成的第 2 分离数据结合来形成上述数据传送键;

上述接收机还包括:

接收加密的上述第 2 分离数据的第 3 接收机构;

对所接收的上述第 2 分离数据进行译码的第 3 译码机构;

第 2 比较机构，该机构对译码的上述第 2 分离数据和上述第 2 随机数进行比较，在它们保持一致的场合，认证上述发送机为正当的设备;

第 2 数据传送键形成机构，在进行上述认证的场合，该机构通过将借助上

述第 1 译码机构形成的上述第 1 随机数和借助上述第 2 随机数形成机构所形成的第 2 随机数结合来形成上述数据传送键;

上述发送机还包括:

第 4 加密机构，该机构采用通过上述第 1 数据传送键形成机构形成的数据传送键对传送数据进行加密;

将加密的传送数据发送给上述接收机的第 4 发送机构;

上述接收机还包括:

从上述接收机接收加密的上述传送数据的第 4 接收机构;

第 4 译码机构，该机构采用通过上述第 2 数据传送键形成机构形成的数据传送键对传送数据进行译码。

说　　明　　书

保证设备之间通信安全的加密装置

本发明涉及设置于通信设备中的加密装置，该通信设备采用共同的秘密键进行密码通信，本发明特别涉及可通过较小的电路规模进行工作的加密装置。

目前有很多下述的场合，该场合指需要防止通过通信线路进行通信的数据在通信线路上被非法复制或修改。

该场合指下述的场合，如将图象等作品进行数字化处理并进行信息压缩，接着将其以数字方式记录于光盘上，通过光盘再生装置将其作为电信息取出，通过信息扩展装置将所取出的数字信息扩展，通过图象声音再生装置将其再生。

这里，在光盘再生装置和信息扩展装置作为单独的装置分开、并且在它们之间通过数字通信线路进行数据通信的场合，如果在未经著作权人许可的情况下，通过数字信息记录装置记录上述通信数据，之后通过数字信息复制装置复制该数据，则便产生对该图象作品的非法复制，从而发生著作权受到侵害的情况。因此，必须防止在通信线路上非法复制通过通信线路通信的数据。由于设备内部的电路或部件的规格一般是不公开的，而数据通信用的电特性或信号形式一般是公开的，这样就会产生通信线路中的数据的非法复制或由此连续的数据修改的严重问题。

关于排除上述非法行为确保安全通信用的技术，过去人们知道有各种。

最具代表性的为采用对方认证方法的技术。该技术通过下述的方式防止数字作品为非法设备所接收，该方式为：一般是在数据发送一侧认证接收一侧的正当性，仅仅在确认是正当接收者时，才发送数据。

按照此场合中的接收者，把证明自己的正当性的一侧称为证明侧，另外按照此场合中的发送者，把确证对方的正当性的一侧称为认证者。此外，在与上述光盘记录再生装置有关的设备的这种场合，由于还有在特定设备之间是否实现认证的情况，这样会产生下述的问题，即这些设备是否符合与光盘有关的设备制造领域所确定的规格。因此，在上述的场合，“正当性”意味着“符合所定的规格”。

（第 1 已有技术）

作为第 1 种具体的已有技术，具有采用记载于国际标准规格 ISO/IEC9798-2 中的密码技术的单向认证方法。

该认证方法的基本内容是：证明者具有称为认证键的秘密数据，在不知道该键本身的情况下对认证者要进行证明。为此，首先认证者选择某一数据，之后将其传送给证明者。把这种行为称为询问、发送的数据称为询问数据。

与此相对，证明者采用预先所具有的密码变换和认证键对上述询问数据进行加密。之后，将该加密的数据返还给认证者。该行为称为响应，该数据称为响应数据。

接收了该响应数据的认证者共同采用构成证明者所具有的密码变换的逆变换的译码变换和认证键，并采用上述认证键和译码变换对由证明者返回的响应数据进行译码。如果该结果与上述询问数据保持一致，对接收者是否具有正当认证键进行判断，从而对证明者的正当性进行认证。单向认证表示其中一侧向另一侧证明其正当性。

在这里，密码变换 T 为从由键数据 S 所定的平常文字集合向密码文字集合的映像。当平常文字为 X 时，则将密码文字写为 T （ S， X ）。同样，在从由同一键数据 S 所定的密码文字集合向平常文字集合的映像即逆变换 TINV 之间，具有下述的关系，该关系为:

TINV （ S， T （ S， X ））＝ X

其含义是：对平常文字 X 进行密码变换，当对其进行逆变换时，则返回原始状态。密码变换的逆变换称为译码变换。为了进行密码变换，必须在不知道键 S 时，根据 T （ S， X ）求出 X，但这是困难的。另外，按照惯例，将密码变换称为 E （ S， ），将译码变换称为 D （ S， ）。

图 1 为表示记载于上述规格中的认证方法的一个实例的示意图。

该图 1 表示从第 1 设备 11 向第 2 设备 12 传送数字作品 mj 的场合。在这里，第 1 设备 11 确认第 2 设备 12 的正当性。

下面按照在图 1 中所表示的步骤标号对上述已有的单向认证方法的动作进行说明。

（ 1 ）第 1 设备 11 形成随机数 R1 。之后，将其作为询问数据通过通信线路发送给第 2 设备 12 。

（2）第2设备12在接收到该随机数时，将存储于第2设备12中的秘密认证键S用作密码键，对上述随机数进行加密。接着，将上述结果C1作为响应数据，通过通信线路发送给第1设备11。

（3）第1设备11在接收到上述响应数据时，将存储于上述第1设备11中的认证键S用作译码键，对上述响应数据C1进行译码。

（4）第1设备11将译码结果RR1与临时保存于第1设备11内部的随机数R1进行比较。当它们一致时，认为第1设备11具有与第2设备12相同的认证键SS，故可认证通信对方是正当的。当它们不一致时，则判断通信对方不是正当的，故中断处理。

（5）第1设备11在认证第2设备12为正当的设备后，通过通信线路将数字作品发送给第2设备12。

假使在通信线路中连接有不具有认证键S的第3设备以便代替第2设备12的场合，则该第3设备不能在步骤（2）中形成正确的值的数据C1，其结果是，由于在步骤（3）中，译码的结果RR1与上述R1不一致，这样在步骤（4）中，第1设备11不会将数字作品发送给该第3设备。

如果在第1设备11和第2设备之间，没有经常采用相同的询问数据和响应数据，则可认为知道该情况的非法的第3设备完全成为第2设备12。为了避免该情况，第1设备11每次发送出不同的询问数据（随机数）。

（第2已有技术）

但是，在上述第1已有技术中，还有可能在认证之后将存储于硬盘装置中的假数据发送给具有正规认证键的第2设备12。为了解决上述问题，在必须是在第1设备11确认第2设备12的正当性的同时，第2设备12也有必要对第1设备11的正当性进行确认。

另外，可认为在双方设备认证之后，在通过通信线路将数字作品传送给第2设备12的过程中，会将上述通信线路上的数据提取，将其存储于例如硬盘等装置中。当然，因此必须具备通信线路上的信号电特性或数据形式等知识，但是由于这些知识一般不是特别秘密的信息，这样从技术上看，很有可能实现上述数字作品的提取。因此，仅仅通过认证是很不够的，必须在实现认证后，有必要在每个设备之间共用随机形成的新键、并进行采用该键对数字作品进行加密且传送的密码通信。另外，在下面，下述的秘密键称为“数据传送键”，该

秘密键指用于对数字作品等可传送的数据进行加密的键。

下面对上述第 1 已有技术的的单向认证进行扩张，对进行双向认证、数据传送键的共用、以及密码通信的第 2 已有技术进行说明。

图 2 为实现该双向认证的装置的示意图。

图 2 表示从第 1 设备 21 向第 2 设备 22 传送经过加密后的数字作品 mj 的场合。

下面根据图 2 所示的步骤标号对上述已有的双向认证、数据传送键的共用的动作进行描述。

（ 1 ）第 1 设备 21 形成随机数 R1 。该随机数 R1 具有第 1 询问数据的意义。之后，通过通信线路将其发送给第 2 设备 22 。

这里随机数 R2 具有从第 2 设备 22 向第 1 设备 21 传送的第 2 询问数据的意义。换言之，密码文字 C1 具有与第 1 询问数据相对应的响应数据以及第 2 询问数据两方面的意义。

（ 2 ）第 2 设备 22 形成随机数 R2 ，通过将该随机数 R2 与由第 1 设备接收的随机数 R1 结合的方式形成结合数据 R1 ‖ R2 。这里符号“‖”表示两种数据沿位数方向并排结合。另外，第 2 设备 22 将认证键 S 作为密码键，将上述结合数据 R1 ‖ R2 加密，将其密码文字 C1 发送给第 1 设备 21 。

（ 3 ）第 1 设备 21 以认证键 S 作为译码键对第 2 设备 22 接收的密码文字 C1 进行译码，使其结果的上位构成分离数据 RR1 ，使该结果的下位构成分离数据 RR2 。

（ 4 ）第 1 设备 21 将该分离数据 RR1 与暂时存储于第 1 设备 21 中的随机数 R1 进行比较。当它们一致时，认证通信对方为具有认证键 S 的正当设备。如果不一致，则中断此处的认证处理。

（ 5 ）第 1 设备 21 产生随机数 K ，将其设定为数据传送键 K 。之后，通过第 1 设备 21 中的认证键 S 对下述的结合数据 RR2 ‖ K 进行加密，该结合数据 RR2 ‖ K 是将上述获得的分离数据 RR2 和上述数据传送键 K 结合得到的，然后将密码文字 C2 传送给第 2 设备 22 。

（ 6 ）第 2 设备 22 采用认证键 S 对第 1 设备接收的密码文字 C2 进行译码，使该译码结果的上位构成分离数据 RRR2 ，使该结果的下位构成分离数据 KK 。

（ 7 ）第 2 设备 22 将上述分离数据 RRR2 与暂时存储于第 2 设备 22 中的

随机数 R2 进行比较。当它们一致时，认证通信对方为具有认证键 S 的正当设备。当它们不一致时，中断此处的认证处理。另一方面，把译码的分离数据 KK 设定为数据传送键 KK 。

（ 8 ）第 1 设备 21 采用上述数据传送键 K 对数字作品进行加密，通过通信线路将其发送给第 2 设备 22 。

（ 9 ）第 2 设备 22 采用上述数据传送键 KK 对其进行译码，从而获得原始的数字作品。

在这里，假定第 1 设备 21 具有正规的认证键 S ，而第 2 设备 22 不具有正规的认证键，则在步骤（ 4 ）中，第 1 设备 21 判断通信对方不具有正规的认证键，从而可中断认证处理。另外，在第 1 设备 21 不具有正规的认证键，而第 2 设备 22 具有正规的认证键的场合，在步骤（ 7 ）中，第 2 设备 22 判断通信对方不具有正规的认证键 S ，从而可中断认证处理。按上述方式，可在防止数字作品流出到非法的设备中的同时，还可防止上述数字作品从非法的设备流入正当的设备。

此外，在第 1 设备 21 以及第 2 设备 22 都具有正规的认证键的场合，在上述认证处理完毕后，在步骤（ 8 ）中，在数字作品在通信线路上进行传送时，即使在对该数字作品以电的方式进行复制、并且存储于数字存储装置中的场合，由于上述数字作品经过加密，上述复制内容为无意义的数字数据，这样仍可有效地对原始的数字作品进行保护。

按上述方式，为在首尾很好地进行采用密码技术的双向认证，所必须的条件是: 存储于第 1 设备 21 和第 2 设备 22 内部的认证键进行非法的行为是不容易知道的。另外必须不能够从外部访问以及不能够修改用于询问数据的随机数的形成部和数据传送键 K 的形成部。

确保这些结构部件的隐匿性的最有效的方法是下述的方法，该方法指将进行上述认证或数据传送键的共用以及密码通信的部分作为 IC 实现。由于需要花费大量的劳力对 IC 进行解析，这样不容易对认证键 S 等进行解读。

但是，由于通过 IC 形成上述第 2 已有技术中的第 1 设备 21 ，这样上述 IC （下面称为“加密 IC ”）就必须设有下述的部分。

形成随机数 R1 的随机数形成部;

对密码文字 C1 进行译码的译码部;

存储认证键 S 的部分;

对随机数 R1 和分离数据 RR1 进行比较的比较部;

形成数据传送键 K 的随机数形成部;

将分离数据 RR2 和数据传送键 K 结合并进行加密的密码部;

存储数据传送键 K 的存储部;

采用数据传送键 K 对数字作品进行加密的密码部。

同样在第 2 设备中，也必须有相同程度的硬件。

按上述方式，由于通过 IC 来实现上述已有的认证方式，这样会产生下述的问题，该问题是：由于必须具有 2 个随机数形成部、2 个变换部（译码部和密码部）等非常多的功能，从而电路规模较大，并且最终设备的成本上升。

另外，在上述第 2 已有技术中，用于数据加密的数据传送键 K 形成第 1 设备 21，但是由于与必须进行相互认证的情况相同的原因，最好上述传送键反映形成双方设备的值。

按上述方式，为了保护设备之间的线路，采用将认证等功能或该功能所用的秘密信息封入 IC 内部来实现的方法效果较好。但是，在已有的方法中，由于通过 1 个 IC 来形成相互认证的部分、数据传送键共同采用的部分以及数据加密部分，这样该 IC 的规模非常大，从而造价较高。

因此，本发明的第 1 目的在于提供一种加密装置，它具有较小规模的加密 IC、并且具有用于确保设备之间通信安全所必需的最小功能。

在这里，加密 IC 具有下述的功能。

（1）安全地存储认证键。该认证键 S 不会通过从外部访问的方式改写和读出。

（2）安全地实现数据传送键的共用。该数据传送键不会通过从外部访问的方式改写和读出。

（3）但是，由于在加密 IC 中未包括与通信系统安全性无关的部分，从而可使加密 IC 的规模达到最小。

另外，本发明的第 2 目的在于提供一种密码通信系统，其适合采用规模较小的加密 IC 来实现，并且安全性较高。

为了实现上述第 1 目的，本发明采用权利要求 1 所述的结构。

按上述方式，由于与数据传送键的形成直接相关的第 1 随机数保存于不能

从外部访问的加密 IC 的内部，这样可安全地在每个设备中实现随时间变化的数据传送键的共用，以进行密码通信。另外，由于加密 IC 具有对于确保设备之间通信安全所必需的最小功能，从而其可采用较小的电路来实现。

在这里还可采用权利要求 2 所述的结构。

按上述方式，由于第 3 者不能得知与数据传送键的形成直接相关的第 1 随机数，这样可保持数据传送键的秘密性，比如即使在了解密码算法及其逆变换算法的情况下，仍可维持密码通信。

在这里还可采用权利要求 3 所述的结构。

按上述方式，由于在设备之间相互认证成功时，同时形成正规的数据传送键，这样可提高秘密通信的安全性。

在这里，还可采用权利要求 4 所述的结构。

按上述方式，由于与通信系统安全性无关的部分，即与数据传送键的形成没有直接关系的处理部分设置于加密 IC 外边，这样可防止加密 IC 的规模不必要地增加。

在这里，还可采用权利要求 5， 12 所述的结构。

按上述方式，由于具有对于确保设备之间通信安全所必需的最小功能，这样可获得设有较小规模的加密 IC 的加密装置。

在这里，还可采用权利要求 6 所述的结构。

按上述方式，由于可通过 1 个转换器同时用作传送数据加密机构和第 1 加密装置或译码机构并进行安装，这样可减小加密 IC 的电路规模。

在这里，还可采用权利要求 7 所述的结构。

按上述方式，即使在为了增加传送数据量而反复对其进行加密到任何的程度的情况下，仍可避免下述不利的情况，该情况指为了加密而大大增加数据的传送时间。

在这里，还可采用权利要求 8 所述的结构。

按上述方式，即使对于数据长度量较大的传送数据的密码通信，本发明的加密装置仍可适用。

在这里，还可采用权利要求 9 所述的结构。

按上述方式，可通过简单的逻辑电路实现传送数据加密机构。

在这里，还可采用权利要求 10 所述的结构。

按上述方式，可通过一个转换器同时用作第 1 加密机构和译码机构并进行安装，这样可减小加密 IC 的电路规模。

在这里，还可采用权利要求 11 所述的结构。

按上述方式，可将仅仅采用屏蔽 ROM 形成认证键 S 的场合的缺点以及仅仅采用附加 ROM 形成认证键 S 的场合的缺点相互弥补。

在这里，还可采用权利要求 19 所述的结构。

按上述方式，由于仅仅形成一个随机数，并将其用作认证和数据传送键的形成这两个目的，这样可减小通过加密装置形成随机数的电路规模。

另外，由于在加密 IC 内部形成认证用的随机数、并进行比较处理，这样可提高密码通信的安全性。

为了实现上述第 2 目的，本发明采用权利要求 26， 27， 28 所述的结构。

按上述方式，由于可在发射机和接收机之间进行相互认证、并形成数据传送键，另外与数据传送键的形成直接相关的随机数不按照原样发送接收，此外与数据传送键的形成直接相关的 2 个随机数分别由发送机和接收机提供，这样适合采用规模较小的加密 IC 来实现，并可实现具有高安全性的密码通信。

根据下述表示本发明实施例的附图容易得出本发明的上述目的，其它目的，优点和特征。

图 1 为第 1 种已有技术的单向认证的处理程序图;

图 2 为第 2 种已有技术的双向认证的处理程序图;

图 3 为本发明第 1 实施例的加密装置的处理程序图;

图 4 为表示图 3 所示的第 1 加密 IC54 的硬件结构的方框图;

图 5 为本发明第 2 实施例的加密装置的处理程序图;

图 6 为本发明第 3 实施例的加密装置的处理程序图;

图 7 为本发明第 4 实施例的加密装置的处理程序图;

图 8 为表示图 7 所示的第 1 加密 IC94 的硬件结构的方框图;

图 9 为本发明的加密装置用于具体通信系统中的实例示意图;

图 10 为图 9 所示的光盘驱动器 110 的结构的方框图;

图 11 为设置于上述光盘驱动器 110 内部的电路板的示意图;

图 12 为表示图 9 所示的图象再生装置 111 的结构的方框图。

（第 1 实施例）

图 3 为第 1 实施例的处理程序图，该实施例可在设置有本发明的加密装置的第 1 设备和第 2 设备之间进行相互认证、数据传送键的共用、以及数据的密码通信。

图 3 表示从第 1 设备 51 向第 2 设备 52 传送数字作品 mj 的场合。另外，在图 3 中仅仅示出设置于上述每个设备 51， 52 中的加密装置，而省略了与加密装置不直接相关的其它结构部件（收发部，或数字作品处理系统等）。

从整体上看，第 1 设备 51 中设置的本发明加密装置由 MPU53 和第 1 加密 IC54 构成。

上述 MPU53 由存储有上述加密装置中固有的控制程序的 ROM 、运行该控制程序的广泛使用的微处理器和 RAM 等构成，它进行不与采用共同的数据传送键直接相关的处理（图中的步骤（ 1 ）、（ 7 ））。

第 1 加密 IC54 为单片半导体 IC，它进行与采用共同的数据传送键直接相关的处理（图中的步骤（ 3 ），（ 5 ），（ 9 ），（ 11 ））。

同样，从整体上看，设置于第 2 设备 52 中的本发明的加密装置也由 MPU55 和第 2 加密 IC56 构成。

上述 MPU55 由存储有上述加密装置中固有的控制程序的 ROM 、运行该控制程序的广泛使用的微处理器和 RAM 等构成，它进行不与采用共同的数据传送键直接相关的处理（图中的步骤（ 2 ）、（ 8 ））。

第 2 加密 IC56 为单片半导体 IC，它进行与与采用共同的数据传送键直接相关的处理（图中的步骤（ 4 ），（ 6 ），（ 10 ），（ 12 ））。

此外，在上述实施例中，采用符合数据加密标准（ DES： Data Encryption Standard ）的 64 位块密码算法 E 和其逆变换算法 D 。在下面，将采用密码算法 E 的变换称为“加密”，将采用逆变换算法 D 的变换称为“译码”。

另外，第 1 加密 IC54 仅仅具有密码算法 E，而第 2 加密 IC56 仅仅具有逆变换算法 D 。这是因为如果削减每个加密 IC54， 56 的规模，可保证安全。

下面根据图 3 所示的步骤标号，对第 1 实施例的加密装置的动作进行说明。

（ 1 ）在第 1 设备 51 中的 MPU53 中，形成随机数 R1 （ 32 位），将其存储起来并传送给第 1 加密 IC54 。

（ 2 ）与步骤（ 1 ）相同，在第 2 设备 52 中的 MPU55 中，形成随机数 R2

（32 位），将其存储起来并传送给第 2 加密 IC56 。

（3）在第 1 加密 IC54 中，形成随机数 R3 （32 位），将其存储于从外部不能访问的区域。之后，将在上述 MPU53 中形成的随机数 R1 和上述随机数 R3 结合，通过 E 函数进行加密。

在这里，符号“ | | ”表示 2 个随机数在位数方向上结合而形成 64 位（随机数 R1 形成上位 32 位，随机数 R2 形成下位 32 位）。另外，在加密过程中采用下述的秘密认证键 S，该键 S 预先共同保存于第 1 加密 IC54 和第 2 加密 IC56 中。第 1 加密 IC54 通过第 1 设备 51 的发送部（图中未示出）将上述密码结果 C1 发送给第 2 设备 52 。

（4）与步骤（3）相同，在第 2 加密 IC56 中，形成随机数 R4 （32 位），将其保存于从外部不能访问的区域。之后，将在上述 MPU 中形成的随机数 R2 和上述随机数 R4 结合，通过逆变换算法 D 对其进行译码。在译码过程中采用上述认证键 S 。第 2 加密 IC56 通过第 2 设备 52 的发送部（图中未示出）将上述译码结果 C2 （64 位）发送给第 1 设备 51 。

（5）在第 1 加密 IC54 中，采用上述的 E 函数，通过上述认证键 S 对上述第 2 设备 52 所接收的译码文字 C2 进行加密。之后，所获得的 64 位分成作为上位 32 位的分离数据 RR2 以及作为下位 32 位的分离数据 RR4 。另外，分离数据 RR2 通过第 1 设备 51 的发送部发送给第 2 设备 52 ，分离数据 RR4 存储于第 1 加密 IC54 内部的、从外部访问不到的区域而不向外部输出。

此外，在第 1 加密 IC54 和第 2 加密 IC56 相互为标准的 IC 、并且具有相同的认证键 S 的场合，上述分离数据 RR2 与上述第 2 设备 52 中的 MPU55 形成的随机数 R2 一致，上述分离数据 RR4 与上述第 2 加密 IC56 内部存储的随机数 R4 一致。

（6）与步骤（5）相同，在第 2 加密 IC56 中，采用上述逆变换算法 D ，通过上述认证键 S 对上述第 1 设备 51 所接收的密码文字 C1 进行译码。之后，所获得的 64 位分成作为上位 32 位的分离数据 RR1 以及作为下位 32 位的分离数据 RR3 。另外，分离数据 RR1 通过第 2 设备 52 的发送部发送给第 1 设备 51 ，分离数据 RR3 存储于第 2 加密 IC56 内部的、从外部访问不到的区域而不向外部输出。

此外，在第 1 加密 IC54 和第 2 加密 IC56 相互为标准的 IC 、并且具有相

同的认证键 S 的场合，上述分离数据 RR1 与上述随机数 R1 一致，上述分离数据 RR3 与随机数 R3 一致。

（ 7 ）在下述的场合，认证第 2 加密 IC56 和设置有该第 2 加密 IC56 的第 2 设备 52 为正当的器件，该场合指将在第 1 设备 51 的 MPU53 中通过步骤（ 1 ）所存储的随机数 R1 与上述第 2 设备 52 所接收的分离数据 RR1 相比较，两者保持一致的情况。

（ 8 ）与步骤（ 7 ）相同，在下述的场合，认证第 1 加密 IC54 和设置有该第加密 IC54 的第 1 设备 51 为正当的器件，该场合指将在第 2 设备 52 的 MPU55 中通过步骤（ 2 ）所存储的随机数 R2 与上述第 2 设备 52 所接收的分离数据 RR2 相比较，两者保持一致的情况。

（ 9 ）在第 1 加密 IC54 中，通过将在上述步骤（ 3 ）中所存储的随机数 R3 和上述分离数据 RR4 结合，可形成数据传送键 K 。在这里，形成下述的数据传送键 K （ 64 位），该传送键 K 使随机数 R3 构成上位的 32 位，使分离数据 RR4 构成下位的 32 位。另外，由于上述数据传送键 K 将 2 个随机数结合，故将其称为随时间变化的、即新的随机地形成的键。

（ 10 ）与步骤（ 9 ）相同，在第 2 加密 IC56 中，通过将在上述步骤（ 4 ）中所存储的随机数 R4 和上述分离数据 RR3 结合，可形成数据传送键 K 。在这里，形成下述的数据传送键 K （ 64 位），该传送键 K 使上述分离数据 RR3 构成上位的 32 位，使在上述步骤（ 4 ）所存储的分离数据 R4 构成下位的 32 位。另外，上述数据传送键也为随时间变化的键。

此外，在步骤（ 7 ）和步骤（ 8 ）中的相互认证成功的场合，由于在步骤（ 3 ）中所形成的随机数 R3 与在步骤（ 6 ）中所获得的分离数据 RR3 一致，在步骤（ 4 ）所形成的随机数 R4 与在步骤（ 5 ）中所获得的分离数据 RR4 一致，因此分别在步骤（ 9 ）和在步骤（ 10 ）中所形成的数据传送键 K 保持一致。

（ 11 ）在第 1 设备 51 的的第 1 加密 IC54 中，反复进行下述的处理，即使用在上述步骤（ 9 ）中所获得的数据传送键 K 对 MPU53 发出的分块化的数字作品 mj （ 64 位）进行加密，将所获得的密码文字 Cj 发送给第 2 设备 52 ，直到可传送的全部数字作品的发送结束。

（ 12 ）与步骤（ 11 ）相对应，在第 2 设备 52 的第 2 加密 IC56 中，接收

第 1 设备 51 发送的加密的上述数字作品 Cj （ 64 位），使用在步骤（ 10 ）所获得的数据传送键 K 进行译码，将所获得的数字作品 mmj 传送给 MPU55 。上述译码处理反复进行直至上述数字作品 Cj 全部从第 1 设备 51 发送过来。

按上述方式，通过第 1 实施例的加密装置，可在第 1 设备 51 和第 2 设备 52 之间进行相互认证、数据传送键 K 的共用、以及数据的密码通信。

根据上述描述显然可知，上述第 1 实施例具有下述的特征。

第 1 特征在于：将数据传送键 K 安全地保护于加密 IC 的内部。具体地说，如果采用设置于第 1 设备 51 中的加密装置，则为了形成数据传送键 K 而直接采用的 2 个数据，即随机数 R3 和分离数据 RR4 满足下述的条件。

· 随机数 R3 形成于第 1 加密 IC54 的内部，它不向外部输出，并且保存于从外部不可读到的区域。

· 分离数据 RR4 形成于（分离形成）第 1 加密 IC54 内部，它不向外部输出，并且保存于从外部不可读到的区域。

按照上述方式，由于数据传送键 K 保护于加密 IC 内部，这样即使在所采用的密码算法 E 和其逆变换算法 D 公开的情况下，仍可保证第 1 设备 51 和第 2 设备 52 之间的密码通信的安全性。

第 2 特征在于：设置于加密 IC 内部的电路保持在所需要的最低限度。具体地说，如果采用设置于第 1 设备 51 中的加密装置，则可通过第 1 加密 IC54 以外的电路，即 MPU53 实现下述的处理。

· 形成随机数 R1

· 将随机数 R1 和分离数据 RR1 进行比较

换言之，第 1 加密 IC54 的电路规模按照不必太大的方式配置。上述二个处理与对方设备的认证有关，而与数据传送键 K 的形成没有直接关系。因此，即使在比如通过采用 IC 以外的器件实现上述的处理而造成非正当这样的情况下，仍然不可能发生有利于第 1 设备 51 这样的非正当的情况。另外，相对第 2 设备 52 给出的询问数据 C2 的响应数据 RR2 的形成是在加密 IC 内部进行的。

图 4 为表示第 1 加密 IC54 中的硬件结构的方框图；

第 2 加密 IC56 也按照相同程度的硬件规模实现。

外部 I / F 部 61 是用于从外部访问上述第 1 加密 IC54 内部电路的唯一输入输出接口。

随机数形成部 60 形成 32 位的随机数 R3 。

随机数存储部 62 为存储由随机数形成部 60 形成的随机数 R3 的存储电路。

结合部 63 将存储于随机数存储部 62 中的随机数 R3 作为下位 32 位，将通过外部 I / F 部 61 而输入的 32 位的数据 R1 作为上位 32 位结合起来。

认证键 S 存储部 64 为存储预定的认证键 S 的存储电路。

开关 65， 66 分别为 64 位宽度的 3 路输入 1 路输出多路转换器， 64 位宽度的 2 路输入 1 路输出多路转换器。

E 函数 67 为基于密码算法 E 的加密电路。

开关 68 为 64 位宽度的 1 路输入 3 路输出多路转换器。

分离部 69 将开关 68 输出的 64 位数据分成上位 32 位 RR2 和下位 32 位 RR4 。

数据传送键 K 形成部 59 通过将存储于随机数存储部 62 中的随机数 R3 作为上位 32 位，将通过分离部 69 分离的分离数据 RR4 作为下位 32 位结合起来，形成数据传送键 K 。

数据传送键 K 存储部 70 为存储由数据传送键 K 形成部 59 所形成的数据传送键 K 的存储电路。

下面对图 4 所示的各个组成部分在图 3 所示的各个步骤中的可能动作进行描述。

在图 3 中的步骤（ 3 ）中，随机数形成部 60 形成随机数 R3 ，将其存储于随机数存储部 62 中，结合部 63 将该随机数 R3 与通过外部 I / F 部 61 输入的随机数 R1 结合，通过开关 65 传送给 E 函数 67 。 E 函数 67 从认证键 S 存储部 64 中通过开关 66 接收认证键 S ，采用该认证键将结合部 63 输出的结合数据 R1 ‖ R3 加密，将该加密结果 C1 通过开关 68 和外部 I / F 部 61 输出给第 2 设备 52 。

在图 3 的步骤（ 5 ）和（ 9 ）中，通过外部 I / F 部 61 输入的译码文字 C2 通过开关 65 输入到 E 函数中。该 E 函数 67 从认证键 S 存储部 64 接收认证键 S ，采用该认证键 S 对译码文字 C2 进行加密，通过开关 68 将其传送给分离部 69 。分离部 69 将其分离成分离数据 RR2 和分离数据 RR4 ，分离数据 RR2 通过外部 I / F 部 61 输出到外部，分离数据 RR4 传送给数据传送键 K 形成部 59 。数据传送键 K 形成部 59 通过将存储于随机数存储部 62 中的随机数 R3 与分离部 69 传送出的分离数据 RR4 结合，从而形成数据传送键 K ， 之后将数据传送

键 K 存储于数据传送键 K 存储部 70 中。

在图 3 的步骤（ 11 ）中， E 函数 67 采用存储于数据传送键 K 存储部 70 中的数据传送键 K 对数字作品 mj 进行加密，该数字作品是通过外部 I / F 部 61 和开关 65 输入的，通过开关 68 和外部 I / F 部 61 将其结果 Cj 输出给第 2 设备 52 。

另外，在第 1 实施例中，虽然对随机数或密码文字等具体的位长度或数据结构进行了描述，但是本发明可不必限于上述的情况。比如，在上述步骤（ 5 ）中，将 32 位随机数 R1 和 R2 结合形成 64 位，将其输入 64 密码函数 E 中，求出 64 位密码文字 C1 。该部分也可采用下述的方式，即通过将每个随机数形成 64 位，采用密码函数 E 反复进行 2 次加密，从而形成 128 位的密码文字 C1 。但是在此场合，必须保证难于将密码文字 C1 中的与随机数 R1 相关的部分与 R2 相关的部分分开。上述方法的一种是按照 CBC 模式随连锁变化的密码方法。关于 CBC 模式，在电子通信学会 1986 年，第 70 页，池野信一、小山谦二共著的“现代密码理论”文章中对其进行了具体描述。

另外，虽然在第 1 实施例中，由于第 1 加密 IC54 仅仅设有密码函数 E ，第 2 加密 IC56 仅仅设有其逆函数 D ，从而可削减硬件的规模，但是上述特点本身并不构成本发明的实质。换言之，也可为下述的情况，即其根据这些第 1 加密 IC54 ，第 2 加密 IC56 所容许的电路规模或加密算法的种类等决定，比如它们分别同时具有密码算法 E 和逆变换算法 D ，在对随机数进行加密时采用密码算法，在对对方设备传送的信息进行译码时采用逆变换算法 D 。本发明的特征在于：通过将至少与数据传送键 K 形成直接相关的组成部分制成集成电路，可确保秘密通信的安全性。

另外，在第 1 实施例中，也可在第 1 加密 IC54 内部通过步骤（ 1 ）形成随机数 R1 。由此，不可能将第 1 加密 IC54 用作密码译解器，从而可形成更加安全的加密装置。换言之，在第 1 实施例中，随机数 R1 通过第 1 加密 IC54 的外部形成，第 1 加密 IC54 根据该随机数 R1 输出密码文字 C1 。虽然该密码文字 C1 会受到在第 1 加密 IC54 内部形成的随机数 R3 的影响，但是如果随机数 R3 不是非常随机的值，则有可能将第 1 加密 IC54 作为密码译解器不正当地使用。因此，通过在第 1 加密 IC54 内部形成随机数 R1 ，不可能受到上述的侵入，从而上述加密装置更加安全。

（第 2 实施例）

下面对作为图 3 所示的第 1 实施例中的步骤的变换实例的第 2 实施例进行说明。该实施例的目的、效果与第 1 实施例的相同。另外，其硬件规模也与图 4 所示的第 1 实施例相同．在第 1 实施例中，不是通过对询问数据进行加密，而是通过对响应数据进行加密实现通信的，但是在第 2 实施例中，是通过对询问数据进行加密，而不是通过对响应数据进行加密实现通信的。下面重点对与第 1 实施例的不同点进行说明。

图 5 为第 2 实施例中的加密装置的处理程序图，该第 2 实施例在设置有本发明的加密装置的第 1 设备 71 和第 2 设备 72 之间进行相互认证、数据传送键的共用、以及数据密码的通信。

图 5 表示从第 1 设备 71 向第 2 设备 72 传送数字作品 mj 的场合。

MPU73 和第 1 加密 IC74， MPU75 和 第 2 加密 IC76 与第 1 实施例中的 MPU53 和第 1 加密 IC54， MPU55 和第 2 加密 IC56 相对应，除了处理顺序不同以外，硬件的结构与第 1 实施例中的相同。

下面根据图 5 所示的步骤标号，对第 2 实施例中的加密装置的动作进行描述。

（ 1 ）在第 1 设备 71 的 MPU73 中，形成随机数 R1 （ 32 位），将其存储，并通过第 1 设备 71 中的发送部（图中未示出）发送给第 2 设备 72 。在第 2 设备 72 中，该随机数 R1 传送给第 2 加密 IC76 。

（ 2 ）与步骤（ 1 ）相同，在第 2 设备 72 的 MPU75 中，形成随机数 R2 （ 32 位），将其存储，并通过第 2 设备 72 中的发送部（图中未示出）发送给第 1 设备 71 。在第 1 设备 71 中，该随机数 R2 传送给第 1 加密 IC74 。

（ 3 ）在第 1 加密 IC74 中，形成随机数 R3 （ 32 位），将其存储于从外部不能访问的区域。将接收来自上述第 2 设备 72 的随机数 R2 和上述随机数 R3 结合，通过 E 函数进行加密。在加密时，采用下述的秘密认证键 S ，该认证键 S 预先共同保存于第 1 加密 IC74 和第 2 加密 IC76 中。第 1 加密 IC74 将加密结果 C1 （ 64 位）发送给第 2 设备 72 。

（ 4 ）与步骤（ 3 ）相同，在第 2 加密 IC76 中，形成随机数 R4 （ 32 位），将其存储于从外部不能访问的区域。将接收来自上述第 1 设备 71 的随机数 R1 和上述随机数 R4 结合，通过逆变换算法 D 进行译码。在译码时采用上述的认

证键 S 。第 2 加密 IC76 将译码结果 C2 （ 64 位）发送给第 1 设备 71 。

（ 5 ）在第 1 加密 IC74 中，采用上述 E 函数通过上述认证键 S 对接收来自上述第 2 加密 IC76 的译码文字 C2 进行加密。在所形成的 64 位数据中，上位 32 位形成分离数据 RR1 ，下位 32 位形成分离数据 RR4 。之后，分离数据 RR1 传送给第 1 设备 71 的 MPU73 ，分离数据 RR4 存储于第 1 加密 IC74 内部的从外部不能访问的区域而不向外部输出。

另外，在第 1 ，第 2 加密 IC74 ， 76 相互为正规的 IC 、并保持相同的的认证键 S 的场合，上述分离数据 RR1 与上述第 1 设备 71 的 MPU73 形成的随机数 R1 相同，而上述分离数据 RR4 与第 2 加密 IC76 形成的随机数 R4 相同。

（ 6 ）与上述步骤（ 5 ）相同，在第 2 加密 IC76 中，采用上述逆变换算法 D 通过上述认证键 S 对接收来自上述第 1 加密 IC74 的密码文字 C1 进行译码。在所形成的 64 位数据中，上位 32 位形成分离数据 RR2 ，下位 32 位形成分离数据 RR3 。之后，分离数据 RR2 传送给第 2 设备 72 的 MPU75 ，分离数据 RR3 存储于第 2 加密 IC76 内部的从外部不能访问的区域而不向外部输出。

另外，在第 1 ，第 2 加密 IC74 ， 76 相互为正规的 IC 、并保持相同的的认证键 S 的场合，上述分离数据 RR2 与上述第 2 设备 72 的 MPU75 形成的随机数 R2 相同，而上述分离数据 RR3 与第 1 加密 IC74 形成的随机数 R3 相同。

（ 7 ）在下述的场合，认证第 2 加密 IC76 和包含该第 2 加密 IC76 的第 2 设备 72 为正当的器件，该场合指将在第 1 设备 71 的 MPU73 中所存储的随机数 R1 与上述第 1 加密 IC74 所接收的分离数据 RR1 相比较，两者保持一致的情况。

（ 8 ）与步骤（ 7 ）相同，在下述的场合，认证第 1 加密 IC74 和包含该第 1 加密 IC74 的第 1 设备 71 为正当的器件，该场合指将在第 2 设备 72 的 MPU75 中所存储的随机数 R2 与上述第 2 加密 IC76 所接收的分离数据 RR2 相比较，两者保持一致的情况。

（ 9 ）在第 1 加密 IC74 内部，采用上述随机数 R3 和上述分离数据 RR4 形成数据传送键 K 。在图中，两者的结合便构成数据传送键 K （ 64 位）。

（ 10 ）与上述步骤（ 9 ）相同，在第 2 加密 IC76 内部，采用上述随机数 RR3 和上述分离数据 R4 ，与第 1 加密 IC74 一样形成数据传送键 K 。在图中，两者的结合便构成数据传送键 K （ 64 位）。

（ 11 ）在第 1 设备 71 的第 1 加密 IC74 中，反复进行下述的处理，即使

用在上述步骤（ 9 ）中所获得的数据传送键 K 对 MPU73 发出的分块数字作品 mj（ 64 位）进行加密，将所获得的密码文字 Cj 发送给第 2 设备 72 ，直到可传送的全部数字作品的发送结束。

（ 12 ）与步骤（ 11 ）相对应，在第 2 设备 72 的第 2 加密 IC76 中，接收第 1 设备 71 发送的加密的上述数字作品 Cj （ 64 位），使用在步骤（ 10 ）所获得的数据传送键 K 进行译码，将所获得的数字作品 mmj 传送给 MPU75 。反复进行上述译码处理直至上述数字作品 Cj 全部从第 1 设备 71 发送过来。

按上述方式，通过第 2 实施例的加密装置，和第一实施例的场合同样，可在第 1 设备 71 和第 2 设备 72 之间进行相互认证、数据传送键 K 的共用、以及数据密码的通信。

另外，如上所述，对于本实施例与第 1 实施例的加密装置，它们的硬件结构相同，只是处理顺序，即每个硬件结构组成部分的连接和实现顺序不同。因此，可以说本实施例的加密装置的特征或其变换实例与第 1 实施例的场合相同。

（第 3 实施例）

上述的第 1 实施例和第 2 实施例中的加密装置具有下述的相同点。

（ 1 ）在双方的设备中，分别形成 2 个随机数，其中一个仅仅用于认证，而另一个仅仅用于形成数据传送键 K 。

（ 2 ）用于形成数据传送键 K 的随机数未按原样输出到加密 IC 的外部，而用于认证用的随机数则输出到加密 IC 的外部并公开。

与此相对，下面将要描述的第 3 实施例的加密装置仅仅形成一个随机数，该随机数同时用于认证和形成数据传送键。其原因是：与第 1 和第 2 实施例相比，可减轻加密 IC 内部随机数形成的负担。

另外，在加密 IC 的内部形成用于认证的随机数，并进行比较处理。即，与第 1 和第 2 实施例不同，通过加密 IC 内部电路，不仅形成数据传送键，而且还进行认证处理。其原因是：如上所述，要对付将加密 IC 用于密码译解的不正当使用，从而可提高密码通信的安全性。

图 6 为本发明第 3 实施例的加密装置的处理程序图，该实施例可在设置有本发明的加密装置的第 1 设备 81 和第 2 设备 82 之间进行相互认证、数据传送键的共用、以及数据的密码通信。

图 6 表示从第 1 设备 81 向第 2 设备 82 传送数字作品 mj 的场合。

另外，在本实施例中，与第 1 实施例和第 2 实施例相同，设置于每个设备 81， 82 中的本发明加密装置从整体上看，由 MPU83， 85，以及加密 IC84，86 构成。另外，由于 MPU83， 85 具有仅仅把数字作品 mj 传送给加密 IC84，86 的功能，这样实质上本发明的加密装置仅仅由加密 IC84， 86 构成。

第 1 加密 IC84 和第 2 加密 IC86 与第 1 和第 2 实施例相同，为单片的半导体 IC。

下面根据图 6 所示的步骤标号，对第 3 实施例的加密装置的动作进行描述。

（ 1 ）在第 1 加密 IC84 中，产生随机数 R1，将其存储起来，通过 E 函数对其进行加密，通过第 1 设备 81 中的发送部（图中未示出）将密码文字 C1 发送给第 2 设备 82。在加密过程中，采用与第 2 加密 IC86 预先共同保持的秘密认证键 S。在第 2 设备 82 中，将所接收的密码文字 C1 传送给第 2 加密 IC86。

（ 2 ）在第 2 加密 IC86 中，所接收的密码文字 C1 通过逆变换算法 D 译码，获得译码文字 RR1。在第 1 加密 IC84 和第 2 加密 IC86 为正规部件的场合，上述译码文字 RR1 与上述随机数 R1 保存一致。

（ 3 ）在第 2 加密 IC86 中，产生随机数 R2，将其存储起来，使其与上述译码文字 RR1 相结合，并通过上述逆变换算法 D 译码。在译码过程中采用上述的认证键 S。第 2 加密 IC86 通过第 2 设备 82 中的发送部（图中未示出）将译码文字 C2 发送给第 1 设备 81。在第 1 设备 81 中，将其传送给第 1 加密 IC84。

（ 4 ）在第 1 加密 IC84 中，通过 E 函数对上述译码文字 C2 进行加密，将其分解为分离数据 RRR1 和分离数据 RR2。另外，当分离数据 RRR1 通过正当的设备交换时，上述译码文字 RR1 和随机数 R1 保持一致。另外，分离数据 RR2 与上述随机数 R2 保持一致。

（ 5 ）在第 1 加密 IC84 内部，对通过上述步骤（ 1 ）存储的随机数 R1 和上述分离数据 RRR1 进行比较，当它们保持一致时，对第 2 加密 IC86 以及包括该第 2 加密 IC86 的第 2 设备 82 的正当性进行认证。

（ 6 ）在第 1 加密 IC84 中，通过上述 E 函数对上述分离数据 RR2 进行加密，将其发送给第 2 设备 82。第 2 设备 82 将其密码文字 C3 传送给第 2 加密 IC86。

（7）在第2加密IC86中，通过上述逆变换算法D对上述密码文字C3进行译码，从而获得译码文字RRR2。

（8）在第2加密IC86中，对通过上述步骤（3）存储的随机数R2和上述译码文字RRR2进行比较，当它们保持一致时，对第1加密IC84以及包括该第1加密IC84的第1设备81的正当性进行认证。

（9）在第1加密IC84中，通过将上述随机数R1和上述分离数据RR2结合，形成数据传送键K。

（10）在第2加密IC86中，使用上述译码文字RR1和上述随机数R2形成数据传送键K。

（11）在第1设备81的第1加密IC84中，反复进行下述的处理，即使用在上述步骤（9）形成的数据传送键K对MPU83给出的分块数字作品mj（64位）进行加密，将所形成的密码文字Cj发送给第2设备82，直到可传送的全部数字作品的发送结束。

（12）与步骤（11）相对应，在第2设备的第2加密IC86中，接收第1设备81所发送的加密的上述数字作品Cj（64位），使用在上述步骤（10）形成的数据传送键K并进行译码处理，将所形成的数据作品mmj传送给MPU85。反复进行上述译码处理，直至将上述数字作品cj从第1设备81全部发送过来。

按上述方式，通过第3实施例的加密装置，与第1和第2实施例相同，可在第1设备81和第1设备82之间，进行相互认证、数据传送键K的共用、以及数据密码的通信。

另外，在上述步骤（1），（2），（6）和（7）中进行一个随机数的加密，在步骤（3），（4）中进行2个随机数的结合的加密。在采用64位宽度的E函数和逆变换算法D的场合，也可使每个随机数为32位，在前一情况中，在输入剩余的32位时填充固定的32位值。比如，将随机数定为下位32位，使上位32位全部为固定值零等。另外，对于后一情况，也可将所结合的64位按照原样输入到每个函数中。

此外，在每个随机数的位长度为64位的倍数时，对于前者，也可按照原样输入到函数中，对于后者，也可反复2次采用每个函数，按照CBC的模式进行具有一定连锁性的加密。

在上述第3实施例中，与第1和第2实施例不同，其随机数同时用作认证

的随机数，以及与实现数据传送件共用的随机数。此外，用于认证的随机数的形成或用于认证的比较处理在加密 IC 内部进行。因此，由于随机数没有按原样在加密 IC 的外部出现，这样，相对以加密 IC 作为译解器的侵入来说，可更加安全。另外，由于上述原因，即使每个随机数的位数较少，仍可保证十分安全。

（第 4 实施例）

下面对第 4 实施例的加密装置进行说明。

该加密装置的目的在于减小加密 IC 的尺寸，其与上述第 1 ～ 3 实施例的不同点在于：它采用单向认证，另外数据传送键处于公开状态。但是，上述实施例以下述条件为前题，该条件为：密码算法 E 和其逆变换算法 D 处于秘密状态。

图 7 表示从第 1 设备 91 向第 2 设备 92 传送数据作品 mj 时的处理程序的示意图。

图 8 为表示第 1 加密 IC94 的硬件结构的方框图。

（ 1 ）首先，第 1 加密 IC94 的随机数形成部 101 形成随机数 R1 ，该随机数 R1 同时用作询问数据和数据传送键，之后，将该随机数 R1 存储于随机数存储部 102 中，通过外部 I/F 部 100 将其发送给第 2 设备 92 。

（ 2 ）第 2 加密 IC96 通过预先与第 1 加密 IC94 共同采用的认证键 S ，对所接收的随机数 R1 进行密码处理，之后将所获得的译码文字 C1 发送给第 1 设备 91 。

（ 3 ）在第 1 加密 IC94 中， E 函数 106 采用认证键 S 对通过外部 I/F 部 100 和开关 105 接收的译码文字 C1 进行加密，该认证键 S 与预先存储于认证键 S 存储部 103 中的上述认证键 S 相同。其结果是，所获得的数据 RR1 通过开关 107 传送给比较部 108 ，在这里，将其与存储于随机数存储部 102 中的随机数 R1 进行比较。

（ 4 ）当比较结果保持一致时，由于第 2 设备 92 可认证为正当的设备，这样，比较部 108 可按照下述方式对开关 104 进行控制，该方式为存储于随机数存储部 102 中的随机数 R1 用作数据传送键。

（ 5 ） E 函数 106 采用通过开关 104 给出的随机数 R1 对数据作品 mj 进行加密，该数据作品 mj 是从 MPU93 通过外部 I/F 部 100 和开关 105 给出的。之

后，通过开关 107 和外部 I/F 部 100 将其发送给第 2 设备 92 。

（ 6 ）在第 2 设备 92 的第 2 加密 IC96 中，以步骤（ 2 ）中所接收的随机数 R1 作为数据传送键，对由第 1 设备 91 给出的数据作品 Cj 进行译码处理，之后将所获得的数据作品 mmj 传送给 MPU95 。

按上述方式，在本实施例中，借助比第 1 ～ 3 实施例少的步骤和组成部件，实现认证、数据传送键的共用、以及数据的密码通信。

另外，在本实施例中，由于从第 1 设备 91 发送给第 2 设备 92 的随机数 R1 按照原样用作数据传送键，这样第 3 者很容易得知数据传送键。但是，即使在得知该数据传送键的第 3 者对数据作品 Cj 进行盗用译码处理的情况下，如上所述，由于密码算法 E 和其逆变换算法 D 处于秘密状态，这样上述尝试不会成功。

另外，即使第 3 者通过伪造合适的随机数 R1 而对密码算法进行译解的情况下，由于仅仅随机数形成部 101 可将新的随机数 R1 存储于随机数存储部 102 中，另外不存在下述的机构，该机构指从上述第 1 加密 IC94 的外部将新的随机数 R1 存储于随机数形成部 101 中，这样上述尝试也不会成功。

按上述方式，如果密码算法和其逆变换算法处于秘密状态，则还可通过本实施例的尺寸较小的加密 IC 实现认证、数据传送键的形成、以及密码通信。

此外，在上述第 1 ～ 4 实施例中，用于在加密 IC 中设定认证键 S （存储）的方法最好按下述方式进行。

即，该方法步骤包括：在加密 IC 制造时预先设定部分认证键 S ，其余的认证键 S 在上述加密 IC 制造后写入。具体地说，认证键 S 存储部的一部分由写入有部分认证键 S 的屏蔽 ROM 构成，剩余的认证键 S 由可程序控制地写入的附加 ROM 构成。

由于在仅仅通过屏蔽 ROM 构成的场合，具有下述的缺点，该缺点为：与由于不通过人工形成最终的加密 IC 而具有安全性的情况相反，很容易通过采用逆向工程的芯片解析对设定值进行解析；另外在仅仅通过附加 ROM 构成的场合，与通过逆向工程难于对设定值进行解析的情况相反，通过人工进行设定，会混入错误，造成不正确，这样需要对上述两种场合中的缺点进行弥补。

作为上述第 1 ～ 4 实施例的密码通信中的密码算法的具体实例，也可采用下面的形式。

在发送一侧，将数据作品分割成 64 位块，计算上述数据传送键 K （ 64 位）和每位的异或．将该结果作为密码文字．同样在接收一侧，也可计算所接收的 64 位密码文字和数据传送键 K 的异或。这样，可译码成以前的块。

另外，在数据传送键 K 不为恒定值的情况下，也可采用下述的方法，该方法为：对于每个块，在发送一侧和接收一侧，在相同期间对所采用的数据传送键 K 进行更新。为了进行上述的更新，也可采用上述的 E 函数或逆变换算法 D 。块内部的密码 / 译码也可为前面所述的异或。

此外，在上述第 1 ～ 4 实施例中，对于认证方法，对询问响应型的几种实例进行了说明，但是本发明可不必限于此情况。比如也可采用下述的询问响应型的其它的实例，即通过认证一侧的加密 IC 形成随机数，将其作为询问数据发送，对从证明一侧返送过来的响应数据以及认证一侧所形成的参照用询问数据进行比较。

另外，在上述第 1 ～ 4 实施例中，对采用较小的电路规模安全地进行认证、以及密码通信的技术进行了描述，但是很显然安全程度、以及该安全程度所必须的电路规模在于折衷选择的关系。因此，如果 MPU 或加密 IC 内部可实际设置的电路规模有富余的话，为了实现以下的目的，可通过下述方式来强化密码通信的安全性，该方式为：附加导入可进行数据变换 F （ ）的新的变换机构。

（ 1 ）一种机构为使平常文字的询问数据或平常文字响应数据不流过传送通路的机构。

比如，在图 3 所示的第 1 设备 51 对第 2 设备 52 进行认证的处理程序（步骤（ 1 ）、（ 3 ）、（ 6 ）、（ 7 ））中，按下述方式进行变换。

在步骤（ 6 ）中，第 2 加密 IC56 不将分离数据 RR1 传送给 MPU53 ，而是对该分离数据 RR1 进行所定的变换 F （ ），将所得到的数据 F （ RR1 ）传送给 MPU53 。

在步骤（ 7 ）中， MPU53 不对随机数 R1 和分离数据 RR1 进行比较，对随机数 R1 进行与在步骤（ 6 ）所采用的相同的变换 F （ ），对所得到的数据 F （ R1 ）与第 2 加密 IC56 所给出的数据 F （ RR1 ）进行比较。

按上述方式，由于可避免密码文字 C1 和其平常文字的一部分 RR1 流过传送通路，这样可相对已知的平常文字侵入提高安全性能。

（ 2 ）另一个机构为可不将询问数据按原样用作数据传送键的机构。

比如，在图 7 所示的步骤（ 5 ）中，第 1 加密 IC94 不将随机数 R1 按原样用作数据传送键，而是对该随机数 R1 进行规定的变换 F （），将所得到的数据 F （ R1 ）用作数据传送键。

同样，在步骤（ 6 ）中，第 2 加密 IC96 不将随机数 R1 按原样用作数据传送键，而是对该随机数 R1 进行与上述步骤（ 5 ）中所采用的相同的变换 F （），将所得到的数据 F （ R1 ）用作数据传送键。

按上述方式，可对数据传送键 F （ R1 ）加密，强化密码通信的安全性。

（ 3 ）再一个机构为可使结合处理变得复杂的机构。

比如，在图 3 所示的步骤（ 9 ）中，第 1 加密 IC54 不沿单一的位数方向将随机数 R3 和分离数据 RR4 结合，而是对上述随机数 R3 、分离数据 RR4 进行规定的变换 F （），所得到的数据 F （ R3， RR4 ）作为数据传送键 K 。

同样，在步骤（ 10 ）中，第 2 加密 IC56 不沿单一的位数方向将随机数 R4 和分离数据 RR3 结合，而是对上述随机数 R4 、分离数据 RR3 进行与上述步骤（ 9 ）所采用的相同的规定的变换 F （），所得到的数据 F （ R3， RR4 ）构成数据传送键 K 。

按上述方式，可使数据传送键 K 的形成步骤变得复杂，从而强化密码通信的安全性。

（具体的通信系统的适合实例）

按上述方式，本发明的加密装置具有较小规模的加密 IC ，具有下述功能，该功能指确保设备之间进行通信的安全性所必需的最低功能。因此，本发明的加密装置适合用于进行秘密通信所必需的、并且要求较小体积的通信设备，比如携带式电话机或处理数字作品的多媒体相关设备等。

图 9 是本发明的加密装置适用于具体通信系统的实例示意图，它表示图象等数字作品的再生系统的大致轮廓。

该系统由与上述实施例中的第 1 设备相对应的光盘驱动装置 110 ，与第 2 设备相对应的图象再生装置 111 ，与上述设备相连接的 SCS I 电缆 116 等构成，通过上述光盘驱动装置 110 读出的压缩图象数据经过加密而送入图象再生装置 111 ，从而进行图象再生。

图 10 表示光盘驱动装置 110 的结构方框图。

光盘驱动装置 110 包括：对装置整体进行控制的 MPU124 ， SCS I 控制器

121，该控制器 121 为与图象再生装置 111 进行通信的接口，读出控制部 122，该读出控制部 122 对光学头 125 进行控制，从光盘 115 上读出图象数据并进行控制，加密 IC123，该加密 IC123 与上述第 1 ～ 4 实施例中的第 1 设备的加密 IC 对相应，在认证图象再生装置 111 为正当的设备后，读出记录于光盘 115 上的图象数据，在加密 IC123 中对其进行加密，通过 SCS I 电缆 116 将其传送给图象再生装置 111 。

图 11 为设置于光盘驱动装置 110 内部的电路板的示意图。加密 IC123 为在 1 块硅主板上形成的 LS I，其呈通过塑料模制形成的扁平组件形状。

图 12 为图象再生装置 111 的结构方框图。

图象再生装置 111 包括对装置整体进行控制的 MPU131， SCS I 控制器 130，该控制器 130 为与光盘驱动装置 110 进行通信的接口，加密 IC132，该加密 IC132 与上述第 1 ～ 4 实施例的第 2 设备的加密 IC 对相应，MPEG 解码器 133，该 MPEG 解码器 133 对通过加密 IC132 译码的压缩图象数据进行扩展，AV 信号处理部 134，该 AV 信号处理部 134 将所扩展的图象数据变换为模拟图象信号，并以图象方式输出给阴极射线管 112 和扬声器 114 。

由于本发明的加密装置适合用于这样的图象再生系统，这样可防止记录于光盘 115 上的数字作品受到不正当的复制等，并可期待多媒体相关设备流通市场的健全发展。

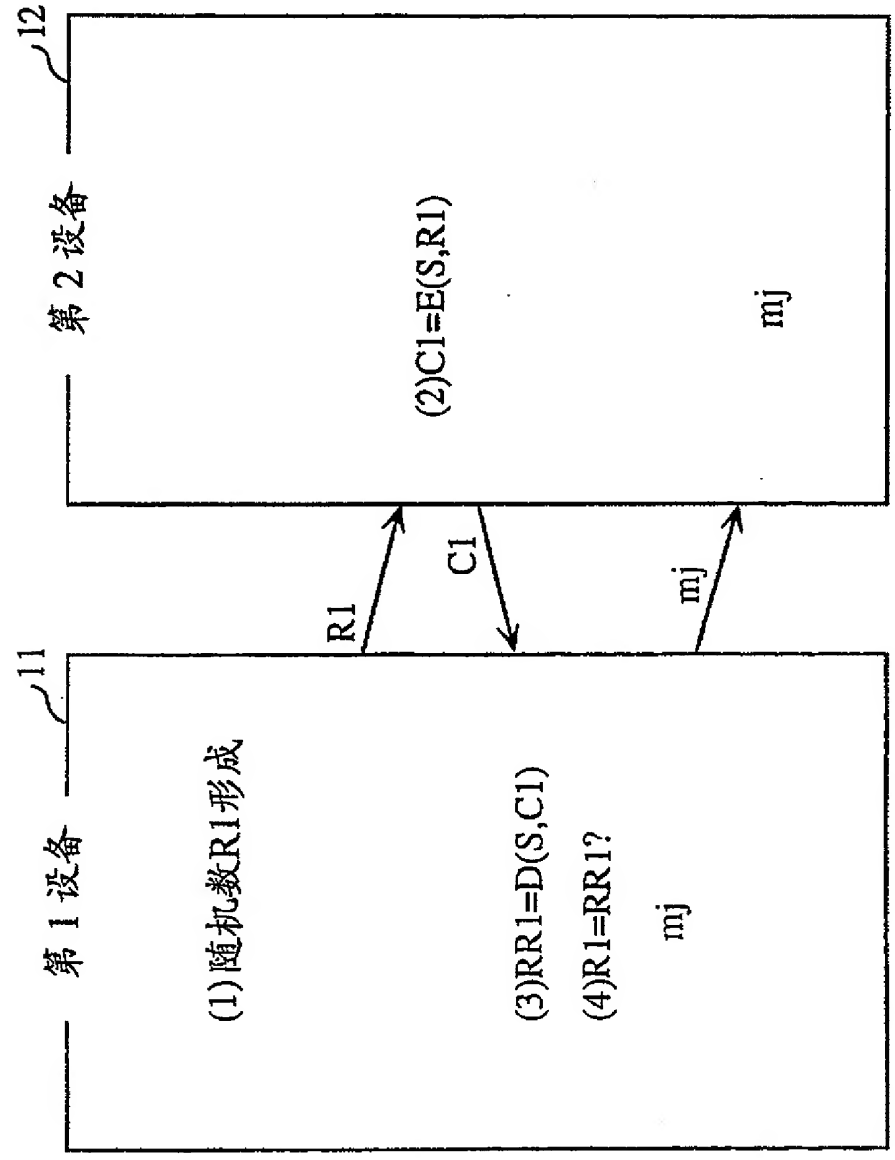

12
第 2 设备
(2)C1=E(S,R1)
mj
R1
C1
mj
11
第 1 设备
(1) 随机数R1形成
(3)RR1=D(S,C1)
(4)R1=RR1?
mj

图　1

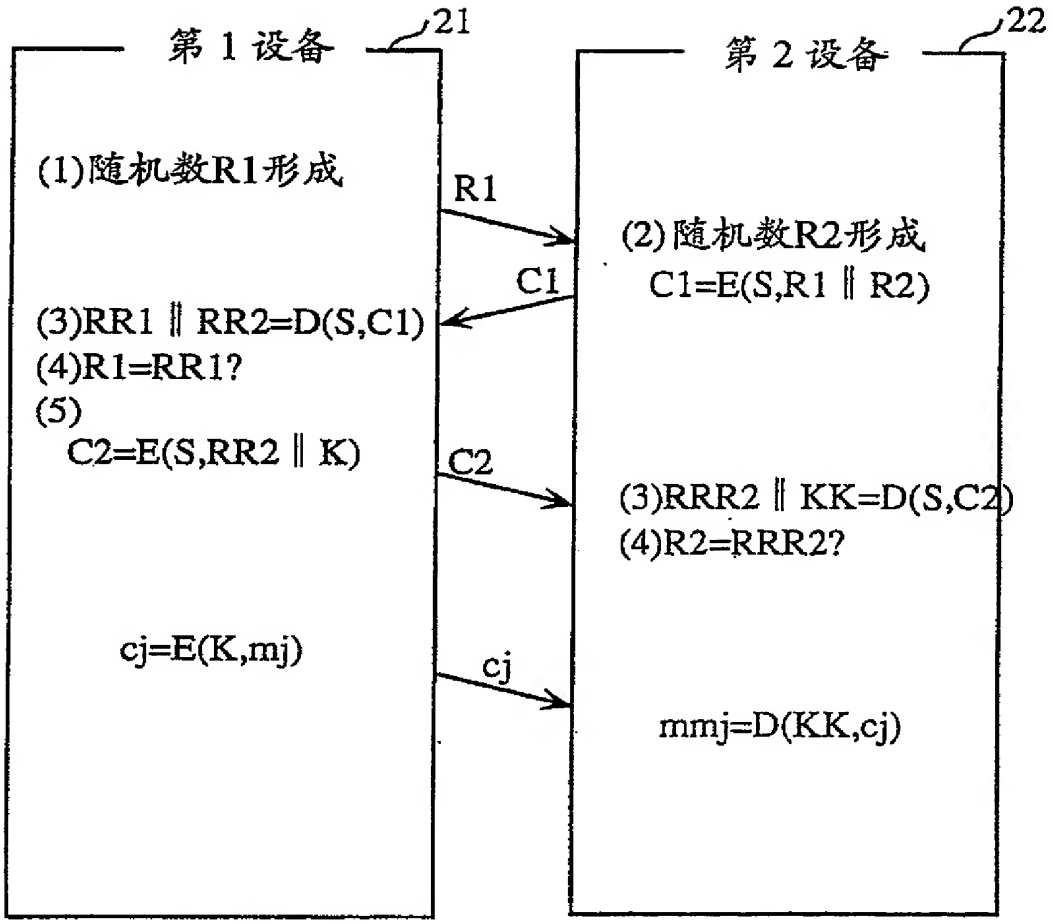

第 1 设备
21
第 2 设备
22
(1)随机数R1形成
R1
(2) 随机数R2形成
C1=E(S,R1 ‖ R2)
C1
(3)RR1 ‖ RR2=D(S,C1)
(4)R1=RR1?
(5)
C2=E(S,RR2 ‖ K)
C2
(3)RRR2 ‖ KK=D(S,C2)
(4)R2=RRR2?
cj=E(K,mj)
cj
mmj=D(KK,cj)

图 2

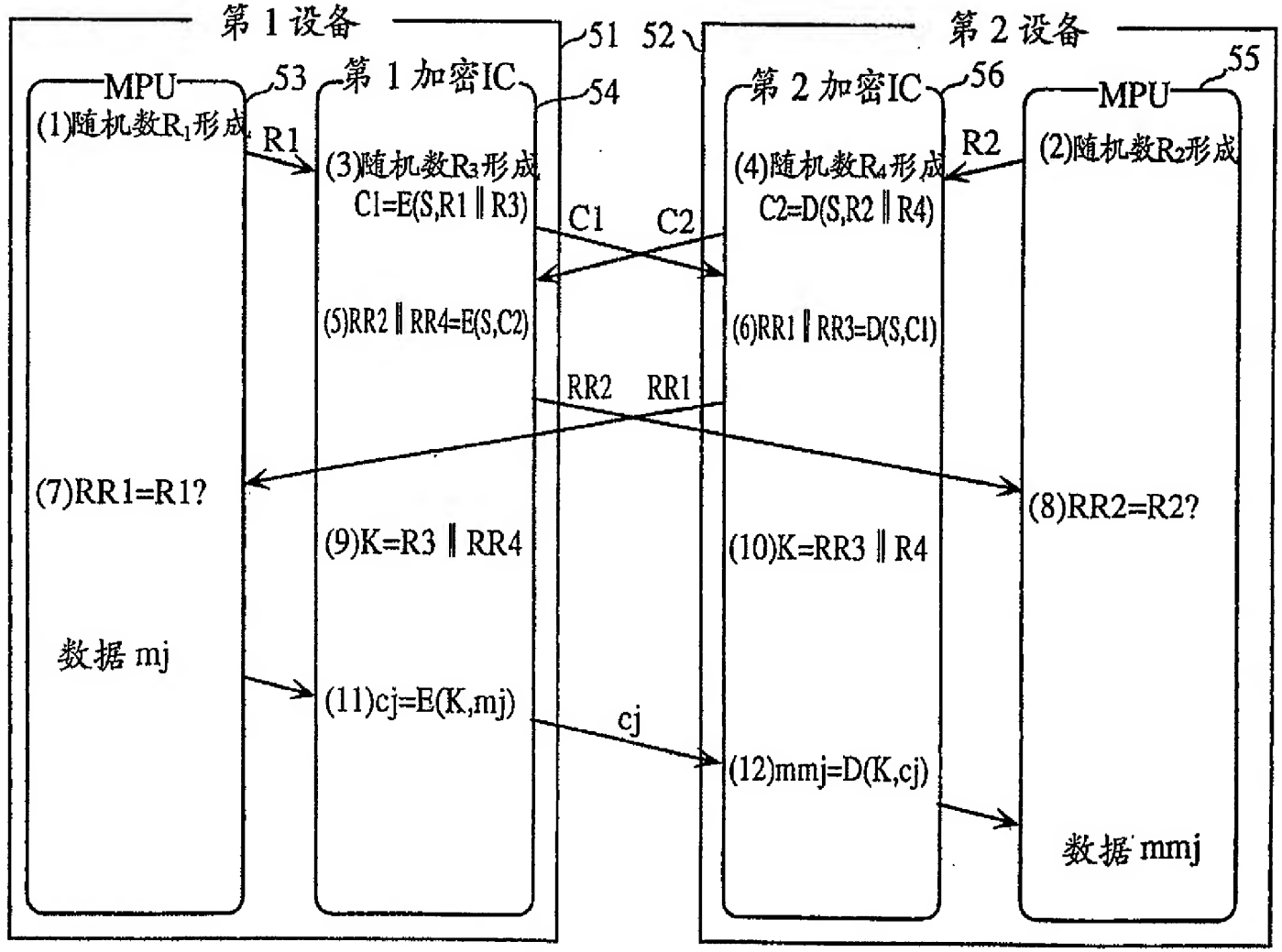

第 1 设备
51
52
第 2 设备
MPU
53
第 1 加密IC
54
第 2 加密IC
56
MPU
55
(1)随机数R1形成
R1
(3)随机数R3形成
C1=E(S,R1 ‖ R3)
C1
C2
(4)随机数R4形成
C2=D(S,R2 ‖ R4)
R2
(2)随机数R2形成
(5)RR2 ‖ RR4=E(S,C2)
(6)RR1 ‖ RR3=D(S,C1)
RR2
RR1
(7)RR1=R1?
(8)RR2=R2?
(9)K=R3 ‖ RR4
(10)K=RR3 ‖ R4
数据 mj
(11)cj=E(K,mj)
cj
(12)mmj=D(K,cj)
数据 mmj

图 3

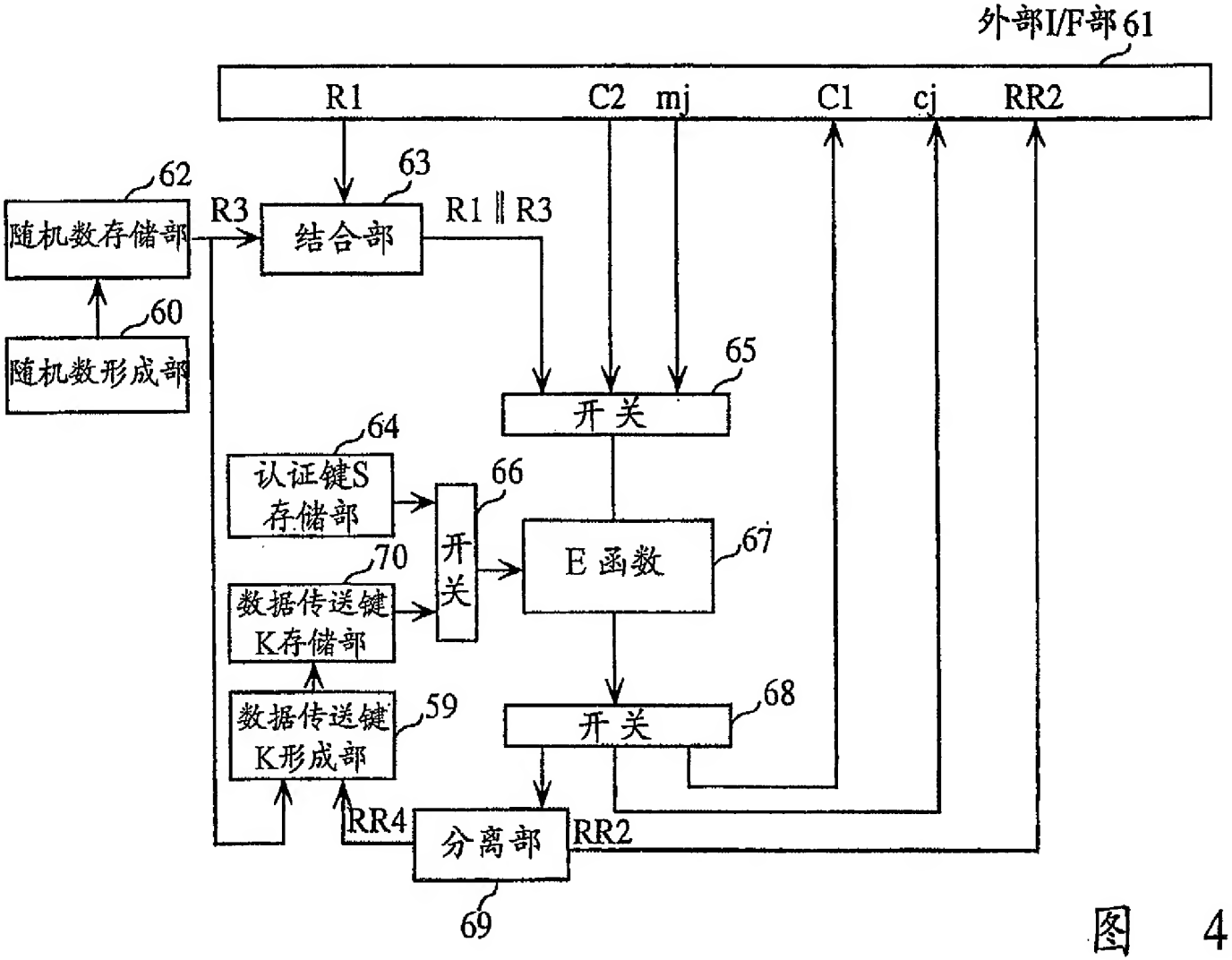

外部I/F部61
R1
C2
mj
C1
cj
RR2
62
随机数存储部
R3
63
结合部
R1‖R3
60
随机数形成部
65
开关
64
认证键S
存储部
66
开关
70
数据传送键
K存储部
E函数
67
数据传送键
K形成部
59
开关
68
RR4
分离部
RR2
69

图 4

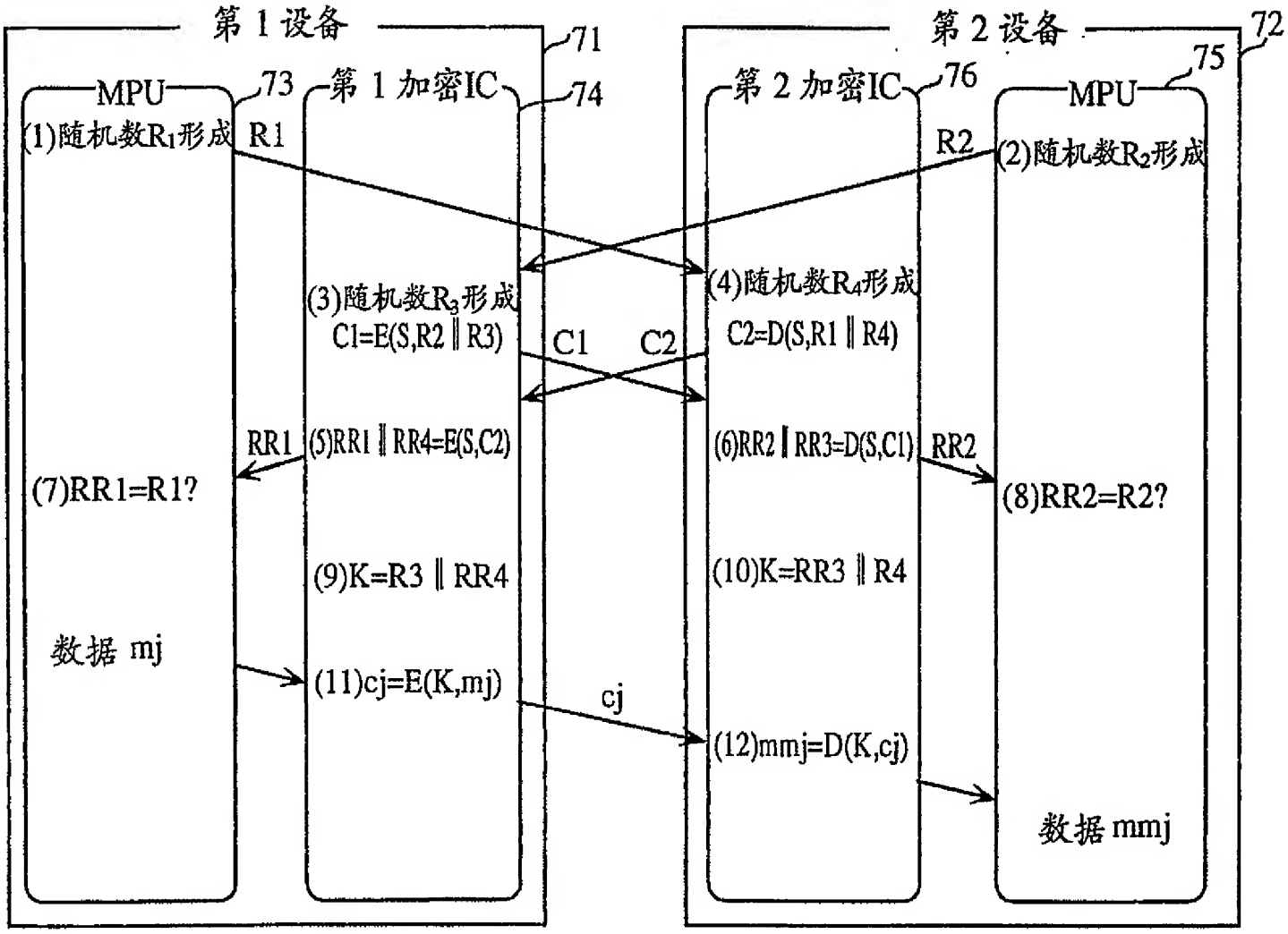

第 1 设备
71
第 2 设备
72
MPU
73
第 1 加密IC
74
第 2 加密IC
76
MPU
75
(1)随机数R1形成
R1
R2
(2)随机数R2形成
(3)随机数R3形成
C1=E(S,R2 ‖ R3)
C1
C2
(4)随机数R4形成
C2=D(S,R1 ‖ R4)
RR1
(5)RR1 ‖ RR4=E(S,C2)
(6)RR2 ‖ RR3=D(S,C1)
RR2
(7)RR1=R1?
(8)RR2=R2?
(9)K=R3 ‖ RR4
(10)K=RR3 ‖ R4
数据 mj
(11)cj=E(K,mj)
cj
(12)mmj=D(K,cj)
数据 mmj

图 5

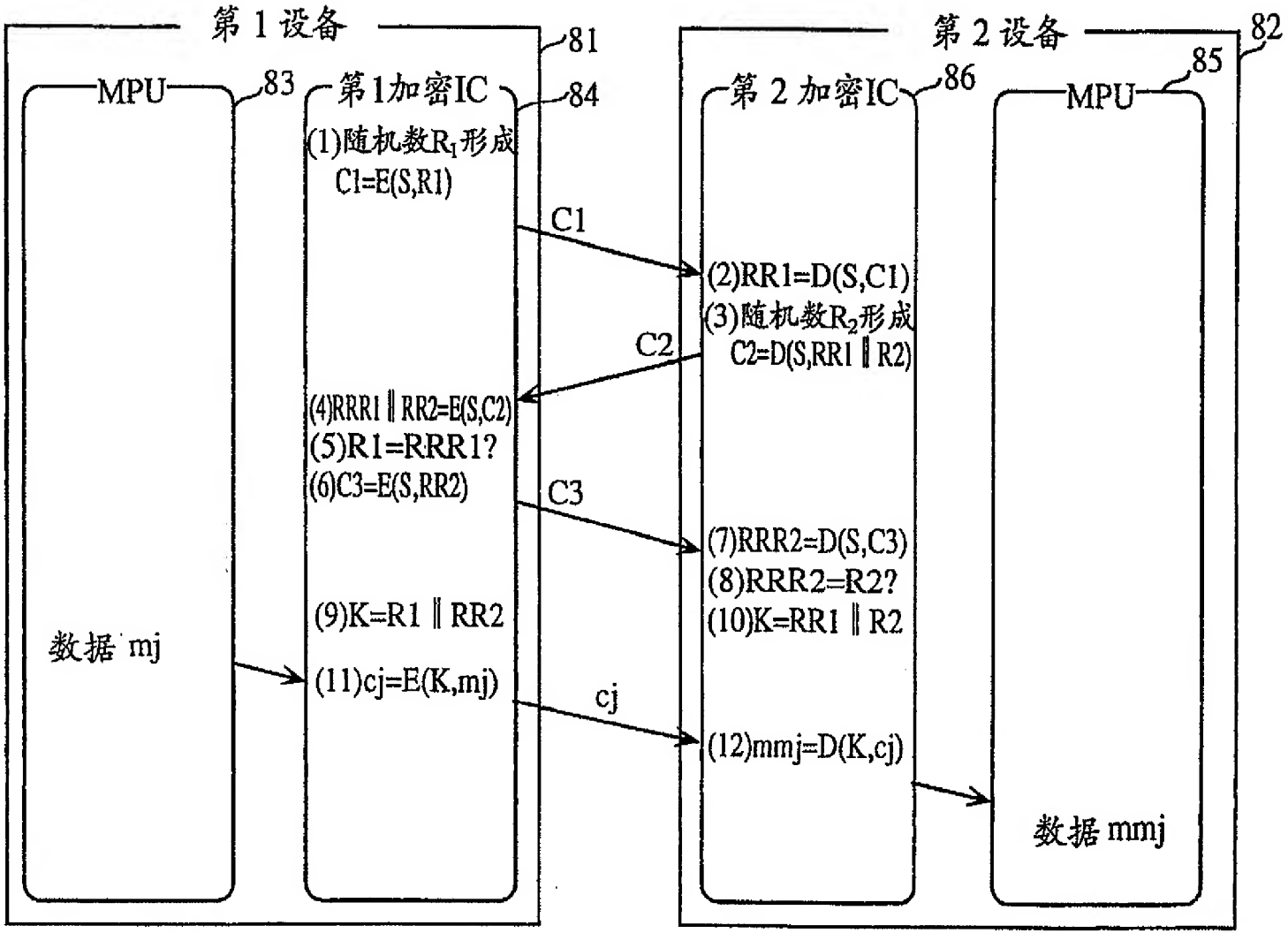

第 1 设备
81
MPU
83
第1加密IC
84
(1)随机数R_1形成
C1=E(S,R1)
C1
C2
(4)RRR1 ‖ RR2=E(S,C2)
(5)R1=RRR1?
(6)C3=E(S,RR2)
C3
(9)K=R1 ‖ RR2
数据 mj
(11)cj=E(K,mj)
cj
第 2 设备
82
第 2 加密IC
86
MPU
85
(2)RR1=D(S,C1)
(3)随机数R_2形成
C2=D(S,RR1 ‖ R2)
(7)RRR2=D(S,C3)
(8)RRR2=R2?
(10)K=RR1 ‖ R2
(12)mmj=D(K,cj)
数据 mmj

图 6

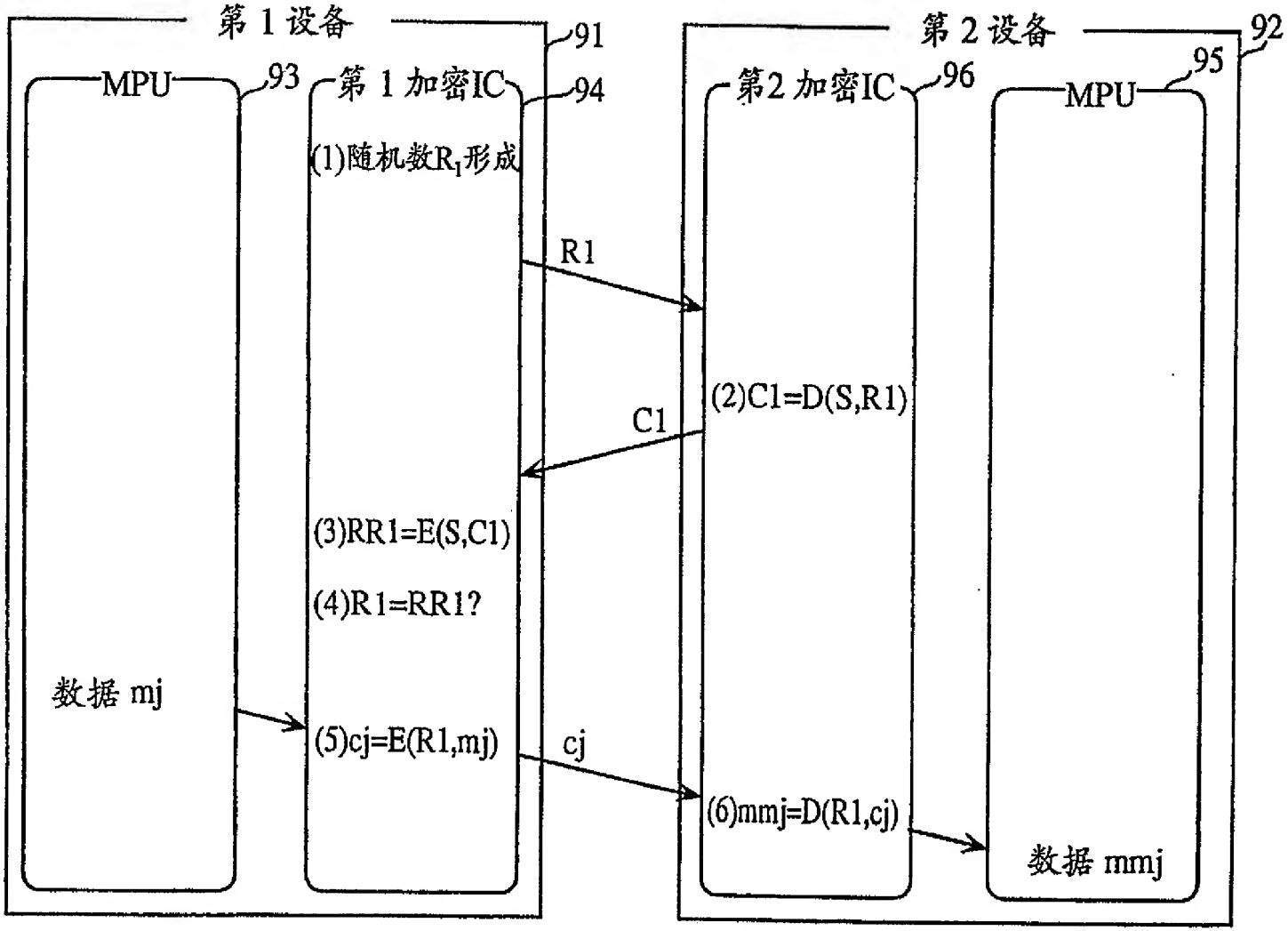

第 1 设备
91
MPU
93
第 1 加密IC
94
(1)随机数R_1形成
R1
C1
(3)RR1=E(S,C1)
(4)R1=RR1?
数据 mj
(5)cj=E(R1,mj)
cj
第 2 设备
92
第2 加密IC
96
MPU
95
(2)C1=D(S,R1)
(6)mmj=D(R1,cj)
数据 mmj

图 7

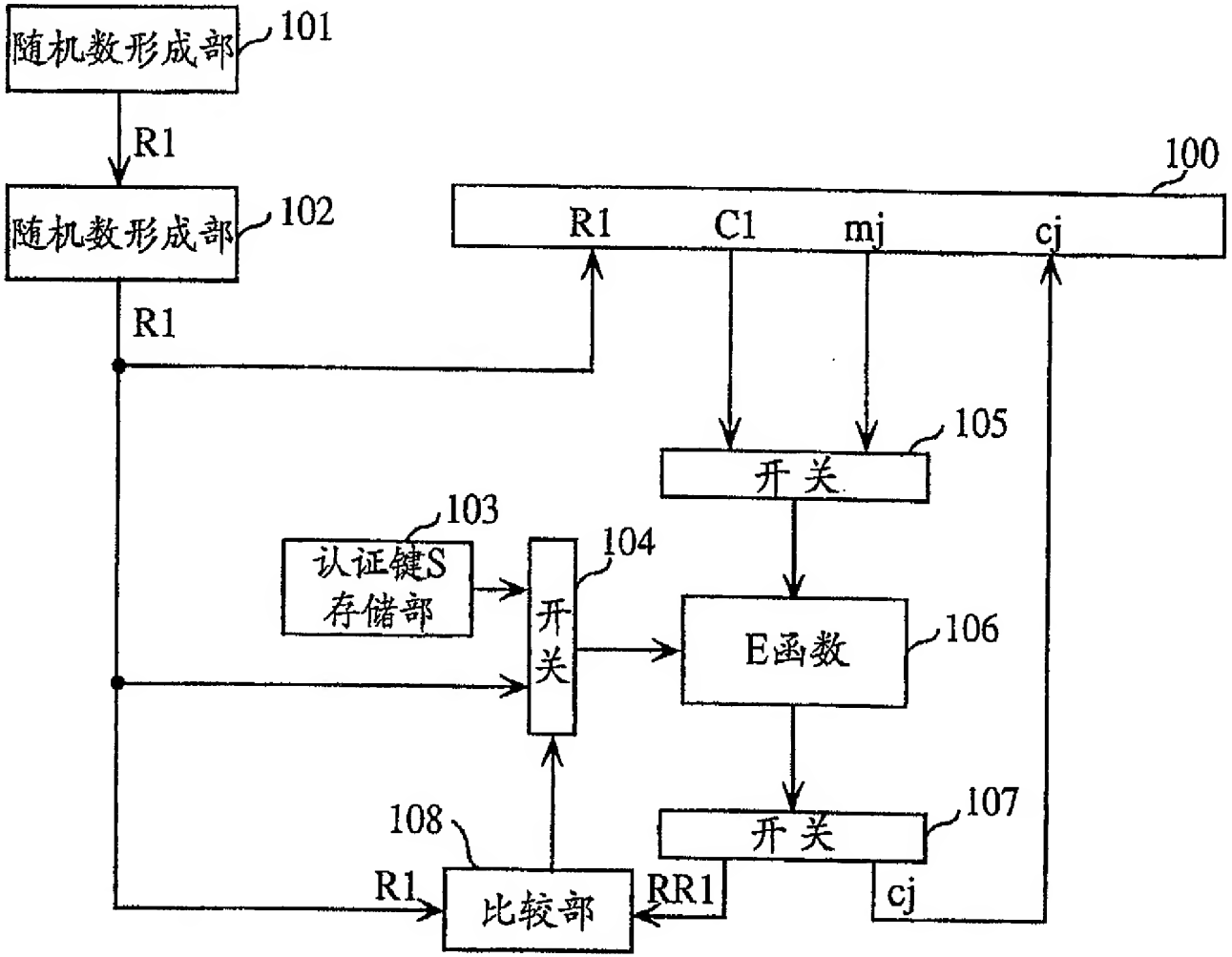

随机数形成部
101
R1
随机数形成部
102
R1
100
R1
C1
mj
cj
105
开关
103
认证键S
存储部
104
开关
E函数
106
开关
107
108
R1
比较部
RR1
cj

图 8

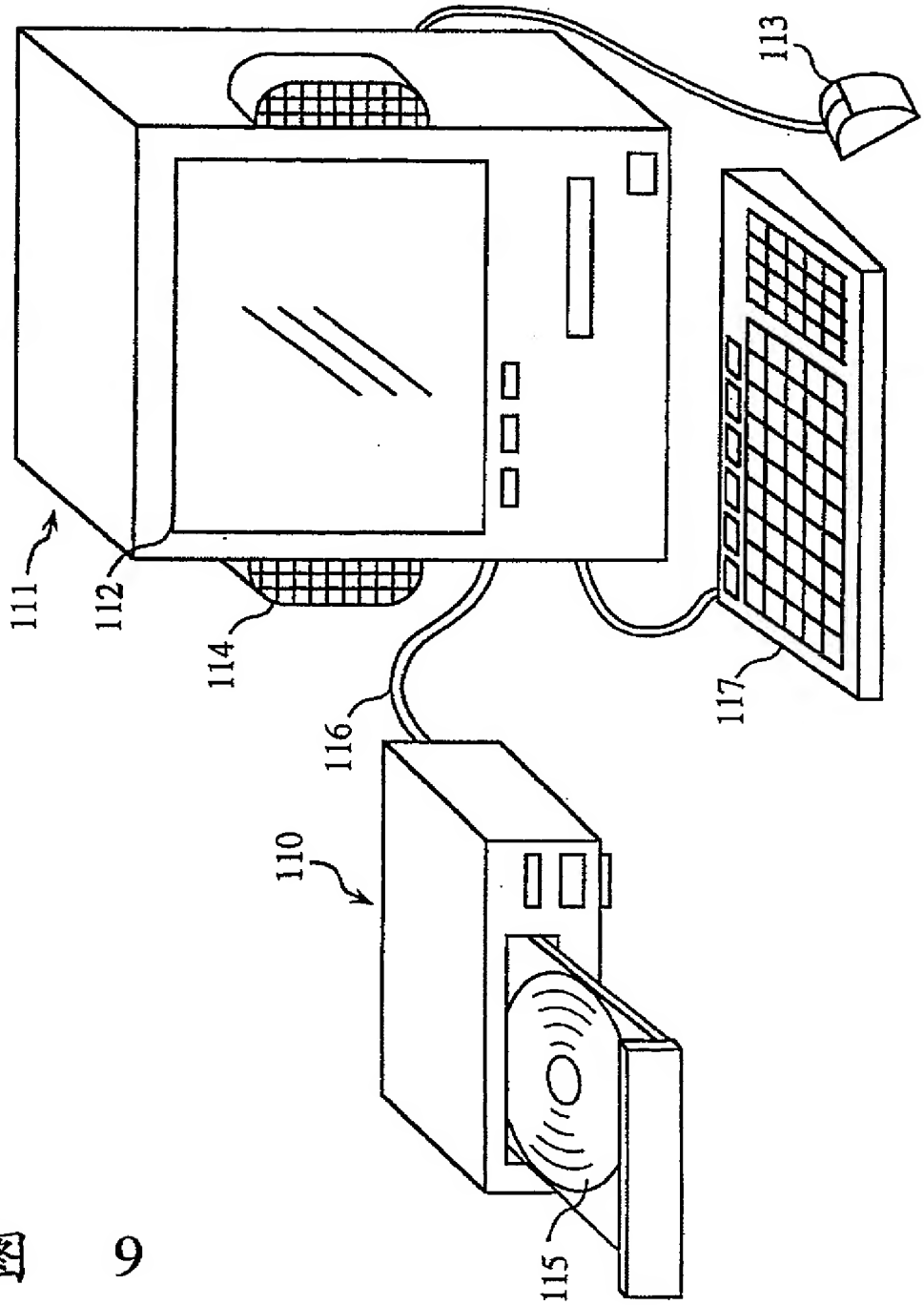


图 9

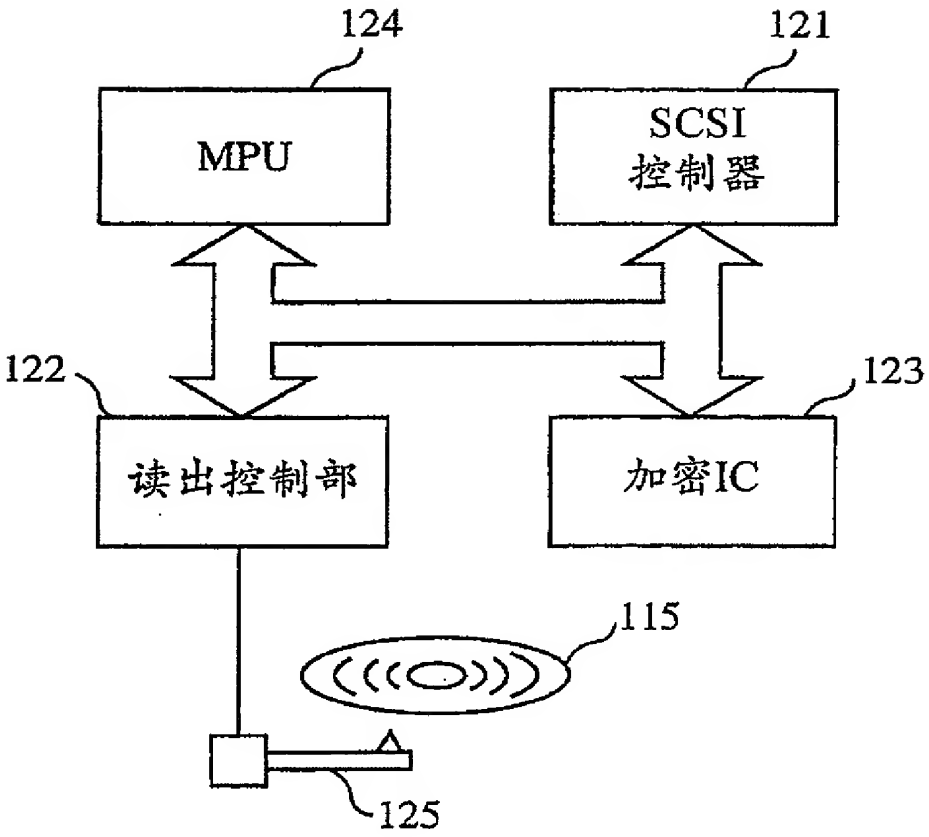


图 10

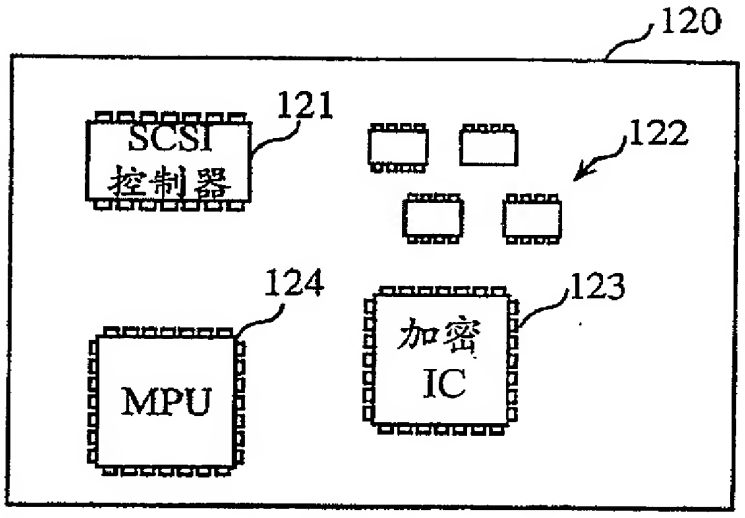

120
121
SCSI
控制器
122
124
MPU
123
加密
IC

图 11

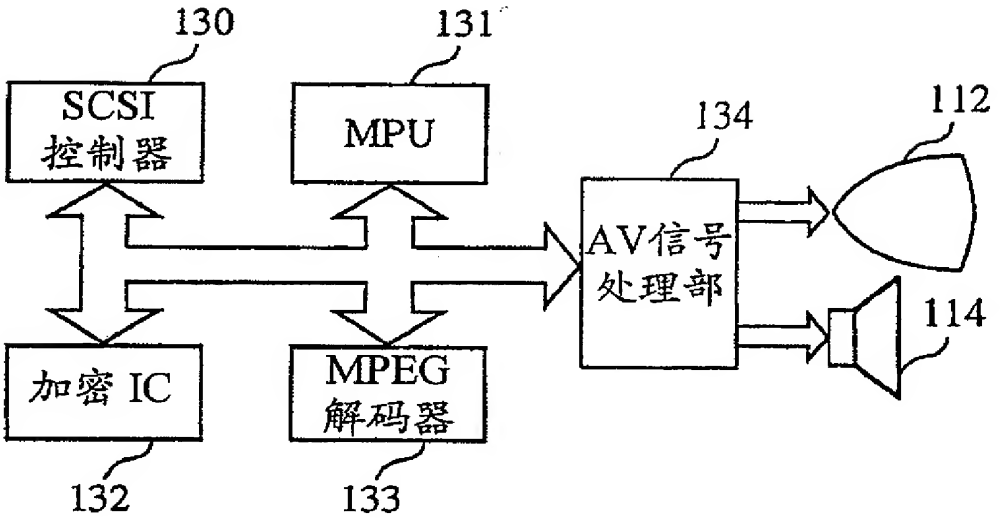

130
SCSI
控制器
131
MPU
134
112
AV信号
处理部
114
加密 IC
MPEG
解码器
132
133

图 12